ssistant Secretary of Defense for
Command, Control, Communications, and
Intelligence (703) 746-7918

DoD 7740.1-G

DEPARTMENT OF DEFENSE

ADP INTERNAL CONTROL

GUIDELINE

JULY 1988

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
(COMPTROLLER)

50272-101

REPORT DOCUMENTATION PAGE	1. REPORT NO. DoD 7740.1-G	2.	3. Recipient's Accession No
4. Title and Subtitle Department of Defense ADP Internal Control Guideline			5. Report Date July 1988 6.
7. Author(s) C. Cardiff			8. Performing Organization Rept. No.
9. Performing Organization Name and Address Assistant Secretary of Defense (Comptroller) Washington, D. C.			10. Project/Task/Work Unit No. 11. Contract(C) or Grant(G) No. (C) (G)
12. Sponsoring Organization Name and Address			13. Type of Report & Period Covered Guide 14.
15. Supplementary Notes			

16. Abstract (Limit: 200 words)

This Guideline provides the means to implement an automatic data processing (ADP) internal control program. The Department of Defense is allocating about $8 billion annually on Automated Information Systems (AIS), is making AIS Life-Cycle Management (LCM) decision which involve multiples of that amount, and is acquiring, fielding, operating and maintaining AISs that are critical to our national security and defense. It is therefore important that the Department of Defense promote and maintain a strong and viable internal control program on ADP.

17. Document Analysis a. Descriptors

b. Identifiers/Open-Ended Terms

c. COSATI Field/Group

18. Availability Statement Release unlimited. For sale by the National Technical Information Service	19. Security Class (This Report) UNCLASSIFIED	21. No. of Pages
	20. Security Class (This Page) UNCLASSIFIED	22. Price

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-1100

COMPTROLLER
Information Resources
Management

FOREWORD

The DoD is allocating about $8 billion annually on Automated Information Systems (AISs), is making AIS Life-Cycle Management (LCM) decisions which involve multiples of that amount, and is acquiring, fielding, operating and maintaining AISs that are critical to our national security and defense. It is therefore important that the DoD promote and maintain a strong and viable internal control program on automatic data processing (ADP) systems. This Guideline provides the means to implement an ADP internal control program and is issued under the authority of DoD Directive 7740.1, "DoD Information Resources Management Program," June 20, 1983.

In November 1984, the first DoD ADP Internal Control Guideline was published. It provided a broad range of ADP internal management control techniques, as well as a series of applicable questionnaires to be used in conducting vulnerability assessments. Much has been learned since the initial publication.

The revised Guideline builds on these lessons, incorporates the latest Office Management and Budget guidance, applies LCM phasing, and provides managers and users with the background and knowledge needed to continue implementing a successful ADP Internal Management Control Program.

Send recommended changes for this Guideline to the Director for Policies and Standards, Office of the DASD(IRM), OASD(C), Washington, D.C. 20301-1100.

DoD Components may obtain copies of this Guideline through their own publication channels. Other Federal agencies and the public may obtain copies from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

John P. Springett
Deputy Assistant Secretary of Defense

ADP INTERNAL CONTROL GUIDELINE
TABLE OF CONTENTS

CHAPTER 6 - INTERNAL CONTROL TECHNIQUES

APPENDIX - LIFE CYCLE MANAGEMENT-INTERNAL CONTROL TECNIQUES

REFERENCES

(a) House Report 99-744, "Implementing the Federal Mangers' Financial Integrity Act - Three Years Later," August 5, 1986

(b) Public Law 97-225, 31 U.S.C. 66a Federal Managers' Financial Integrity Act of 1982," September 8, 1982

(c) OMB Circular A-123 (Revised), "Internal Control Systems," August 4, 1986

(d) OMB Circular A-127, "Financial Management Systems," December 19, 1984

(e) OMB Circular A-130, "Management of Federal Information Resources," December 12, 1985

(f) DoD Directive 5010.38, "Internal Management Control Program," April 14, 1987

(g) DoD Directive 7740.1, "DoD Information Resources Management Program," June 20, 1983

(h) OMB Guidelines for the Evaluation and Improvement of Reporting on Internal Control Systems in the Federal Government, December 1982

(i) GAO Policy and Procedures Manual for Guidance of Federal Agencies, Title 2, "Accounting," November 14, 1984

(j) GAO Policy and Procedures Manual for Guidance of Federal Agencies, Appendix I, "Accounting Principles and Standards," October 1984

(k) GAO Policy and Procedures Manual for Guidance of Federal Agencies, Appendix II, "Standards for Internal Controls in the Federal Government," October 1984

(l) Public Law 93-579, "Privacy Act of 1974," December 31, 1974 (5 U.S.C. 552a)

(m) DoD 7935.1-STD, "Automated Data Systems (ADS) Documentation Standards," April 24, 1984, Authorized by DoD Instruction 7935.1 of September 13, 1977

(n) DoD Directive 7920.1, "Life Cycle Management of Automated Information Systems (AIS), June 20,1988

(o) DoD Instruction 7920.2, "Major Automated Information Systems Approval Process," October 20, 1978

(p) DoD Directive 7750.5, "Management and Control of Information Requirements," August 7, 1986

(q) DoD Instruction 7041.3, "Economic Analysis and Program Evaluation for Resource Management," October 18, 1972

(r) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

(s) Title 44, U.S.C. 3301, Definition of Records

(t) General Records Schedule 20, "Electronic Records," April 5, 1988

(u) NARA Bulletin No. 87-5, "Electronic Recordkeeping," February 11, 1987

(v) "Model Framework for Management Control Over Automated Information Systems," Prepared Jointly by the President Council on Management Improvement and the President's Council on Integrity and Efficiency, August 1987

FIGURES

TABLES

CHAPTER 1

INTRODUCTION

A. BACKGROUND

1. The Department of Defense (DoD) depends increasingly on automated information systems (AISs). The Department's general purpose ADP systems are absolutely essential in supporting our everyday missions and business functions in such areas as logistics, finance and accounting, personnel and payroll, and resource management. Although general purpose ADP systems are normally not those used to aim and fire weapons, these systems are used to assign trained personnel to the correct locations, to allocate supplies in a timely fashion, to pay contractor bills for supplies, to provide management information for use in decision-making and many other business-type applications. These systems are vulnerable to fraud, waste, and abuse. A few examples include:

- unauthorized access and disclosure of classified, privacy, and proprietary records and/or data,
- diversion of payments to unauthorized parties,
- use of computers for personal matters, and
- disruption and loss of computerized records and/or transactions.

2. The House of Representatives' Report on "Implementing the Federal Managers' Financial Integrity Act - Three Years Later (House Report 99-744)," (reference (a)), criticized government agencies for inadequate evaluation of AIS internal controls. The Committee on Government Operations stated agency heads should ensure managers are conducting adequate evaluations of internal controls. Evaluations should include accounting systems, operational testing, and documentation.

3. The United States General Accounting Office (GAO) issued a report in December 1985 entitled "Financial Integrity Act - The Government Faces Serious Internal Control and Accounting System Problems" highlighting widespread weaknesses in AIS operations. The report stated AIS controls were generally not evaluated. Evaluations did not fully address general controls, (applying to the overall management of the agency's AIS function) or application controls, (affecting the quality of data origination, input, processing, and output).

4. After 4 years of effort under the Federal Managers' Financial Integrity Act, DoD Components made progress to identify and report internal control weaknesses, and establish plans for corrective action.

B. PURPOSE

1. This edition updates the Guideline published in November 1984. It addresses congressional and GAO concerns and incorporates the provisions of the Federal Managers' Financial Integrity Act of 1982, revised OMB Circular A-123, OMB Circular A-127, and OMB Circular A-130, (references (b) through (e)). It incorporates the Model Framework for Management Control over Automated Information Systems developed by the President's Council on Management Improvement (PCMI) and the President's Council on Integrity and Efficiency (PCIE).

2. The Internal Management Control Program is mandatory. While application of this Guideline can be tailored to meet specific circumstances, DoD Components must ensure that all relevant parts of the program outlined by the guide are implemented.

3. The Guideline is intended to (1) assist managers, users, and developers in conducting risk assessments of automated activities; (2) provide a framework for use in coordinating management control efforts (i.e., control requirements, control areas); and (3) furnish a ready reference of AIS control techniques. Specifically:

a. If you are a manager involved in AIS operations, Chapter 3 provides a set of 55 system control requirements; in Chapter 5, Questionnaire 1 will tell you how to assess risks in your automated systems.

b. If you are a user, Chapter 5, Questionnaire 3 will help you determine if appropriate controls are in place, and Chapter 6, section 3 provides detailed control techniques to be considered.

c. If you are a developer or modifier of automated systems, you would be particularly interested in Chapter 3 for its control requirements, and Chapter 5, Questionnaire 2 for its risk assessment.

C. SCOPE

This Guideline is for use by all DoD Components that:

1. Manage or are otherwise involved in the operation of data centers,

2. Engage in or contract for AIS systems analysis, design, conversion or installation activities; or

3. Are or will be direct users, managers, and administrators of AIS systems including microcomputers, minicomputers, and networks.

D. OBJECTIVES OF THE GUIDELINE

There are six (6) basic objectives:

1. Assist AIS managers and users in understanding their responsibilities and requirements to develop AIS internal management controls as required by OMB Circular A-123 and by the current DoD Directive 5010.38, DoD Directive 7740.1, and DoD Directive 5200.28 (references (c), (f), (g) and (r)).

2. Provide a vehicle for the education and training of managers so they may have a working understanding of AIS internal management controls.

3. Notify components of a requirement for a 5-year Management Control Plan (MCP) to be developed annually.

4. Delineate responsibilities for managers in either monitoring large AIS systems and assets or conducting internal control reviews and alternative reviews, such as internal audits, inspections, investigations, studies, and computer security reviews.

5. Help to ensure that internal controls receive appropriate attention, emphasis, and resources in the automated information system life cycle, to include development, modification, operation and records management concerns.

6. Show managers how to protect their operation by providing AIS internal control techniques and procedures for conducting risk assessments.

E. DEFINITION AND RESPONSIBILITIES FOR AIS INTERNAL CONTROL

1. DEFINITION

a. Internal control is defined as a plan of organization and all of the methods and measures adopted within an agency to safeguard its resources; ensure the accuracy and reliability of its information; ensure adherence to applicable laws, regulations and policies; and to promote operational economy and efficiency.

b. It is important to emphasize that internal controls do not represent a separate function within DoD but are part of each of the functions that DoD Components use to operate their programs and administrative activities.

c. The definition of internal control and the internal control requirements under OMB Circular A-123 (reference (c)) apply to all DoD Components. As part of overall management, AIS internal control considerations fall in three major control areas:

(1) Management Controls - address organization, policies, plans, and procedures from the perspective of the individuals responsible for overall AIS program management.

(2) Operations Controls - address processing carried out within a data center, including the computers dedicated to a specific program, function or process, and are independent of individual computer applications.

(3) Application Controls - address system development activities, as well as data origination, data input, data processing, and data output of specific computer applications.

d. Using the definition of internal control as a foundation, and incorporating the applicable AIS considerations, the following definition of AIS internal control is presented for use within the Department of Defense:

> The steps taken within each DoD program and administrative function consisting of the plan of organization and all of the methods and techniques used to safeguard AIS resources and provide reasonable assurance of the accuracy and reliability of computer-based input, processing and output; ensure the adherence to applicable laws, regulations and policies; and promote the effectiveness, efficiency and economy of AIS operations and systems.

e. This definition of AIS internal control implies certain prime and shared responsibilities in the areas of executive management, data center management, systems development management, user management, and security management. Summarized below are the primary responsibilities of each of these groups within the management, operations and application components of AIS internal control.

2. RESPONSIBILITIES

a. Executive AIS Management. Executive management involves those personnel responsible for AIS policy and program management. The subset that addresses the AIS internal control responsibilities of executive management includes:

- Management Controls

- Participation with the data center manager, systems developers, users and security managers in:

  -- developing strategic and near term AIS plans,

  -- developing policies and standards for AIS operations and applications,

  -- assuring that AIS resources are acquired in the most economical and expeditious manner,

  -- developing an organization, policies, and procedures that assure that AIS resources are safeguarded and that information is accurately and reliably produced.

  -- ensuring that risk assessments and internal management control reviews have been accomplished and that resulting corrective actions have been fully implemented.

- Obtaining the involvement of the internal audit staff to assure that systems are properly developed and implemented.

b. Data Center Management. Data center management has the overall, day-to-day responsibility for the management of the AIS operating environment, consisting of the physical facility, hardware, software, and procedures that control the timely and accurate execution of programs. Data center management is also concerned with the storage and maintenance of data files and has responsibility for the procurement of AIS resources in a timely and economical manner. In some cases, the control responsibility described for systems developers will also apply to data center management. The primary AIS internal control responsibilities of data center management include:

- Management Controls

  - Participation with executive AIS management, systems developers and users in the development of AIS policies and plans, and the justification and acquisition of AIS resources.

- Operations Controls

  - Establishment and maintenance of procedures in the areas of:

    -- work load scheduling,

-- malfunction reporting and preventive maintenance,

-- user billing and charge-back.

- Development of methods and procedures to assure the accuracy and reliability of:

-- systems software, hardware, and data files.

-- communications and network operations.

- Implementation of control procedures to assure that all data received from users is processed.

- Participation with the AIS security manager and system security officer in the establishment and maintenance of AIS security controls to protect AIS resources.

- Participation with Agency records officers to ensure that all data received from users is disposed of under an approved records disposition schedule.

• Application Controls

- Participation with systems developers in specifying and documenting operational requirements for new or significantly modified applications,

- Implementation of instructions for processing applications, including start-up, processing back-up and emergency procedures,

- Participation with the AIS security manager and system security officer in the maintenance of procedures to ensure the proper delivery of outputs and the appropriate labeling and protection of sensitive outputs.

c. Systems Development Management. Managers of systems development are those personnel responsible for conducting the analysis, design, development, conversion, and implementation of an AIS application. The primary AIS internal control responsibilities of systems developers include:

• Management Controls

- Participation with executive AIS management and users in establishing and maintaining a

system development life-cycle methodology, and assigning responsibility for each phase of the cycle.

- Participation with Agency records officers to ensure records management considerations are included in each phase of the cycle.

d. User Management. User management refers to those personnel with the overall responsibility for a specific application, regardless of whether the application is processed by a dedicated computer, general purpose multi-program computer, or microcomputer. The primary AIS internal control responsibilities of this group include:

- Management Controls
  - Participation with executive AIS management, data center management, and systems developers in AIS planning, development of policies and standards for AIS applications, and the justification and acquisition of AIS resources.
  - Participation with executive management and systems developers in establishing and monitoring the system development life cycle.
  - Participation with the AIS security manager and system security officer in the establishment and maintenance of policies and procedures to assure the AIS resources are safeguarded and that output is accurate and reliable.
- Application Controls
  - Participation with systems developers during the system development life cycle to assure that AIS applications meet user requirements and specifications:
    - -- Authorization of data for processing and execution of data origination and input controls to ensure accuracy, completeness, and timeliness of information to be processed;
    - -- Establishment of effective procedures for reviewing and approving systems output for correcting errors.

e. Relationship Among Terms. Since the first DoD ADP Guideline was published in November 1984, various committees,

President's Council on Management Improvement (PCMI) and President's Council on Integrity and Efficiency (PCIE), and work groups, Office of Management and Budget (OMB) and Office of the Secretary of Defense (OSD), have attempted to synthesize for managers, users, and developers, general guidance on how to protect automated information systems operations. They have examined the same problems and issues from several different perspectives. It is, therefore, not surprising that the terms and labels do not agree in every case. The following table attempts to show a general relationship between the various terms.

Table 1-1 RELATIONSHIP AMONG TERMS

	ADMINISTRATIVE CONTROLS	GENERAL CONTROLS	APPLICATION CONTROLS	REQUIRED SYSTEM FUNCTIONS
MANAGEMENT CONTROLS	X			
OPERATIONS CONTROLS		X		
APPLICATION CONTROLS			X	X

CHAPTER 2

SYSTEM CONTROLS

CONCEPTUAL FRAMEWORK

A. INTRODUCTION

1. This chapter presents a conceptual framework for instituting and maintaining information system controls. The control framework consists of three elements:

a. Control requirements - the terms used to explain why controls are needed and/or what their implementation is expected to achieve.

b. Selection and use of control techniques - the definition, selection, and use of control techniques to satisfy the requirements specified.

c. Areas of control - the terms used to describe how and where control techniques are applied to satisfy basic control requirements.

2. The basic structure of the conceptual framework revolves around these three elements. The remainder of this chapter provides a detailed discussion of the framework and its various supplements. As an aid to the reader, a road map of the system control framework can be found in Figure 2-1 on page 2-4.

3. Most control-related activities have traditionally centered on internal control reviews, risk assessments, and audits of existing automated systems and processes. While these types of reviews are needed, they do not necessarily ensure that adequate management controls are built into current and future systems. Additionally, much of what is written for both managers and systems developers is based on the theoretical aspects of controls. The situation existing today can be summarized as follows:

a. Numerous directives require controls over automated systems, and, while they vary in terminology, specificity, and origin, they all have the same basic objectives. These directives point out a need for secure and reliable systems. In spite of these directives, there are a few simple, clear guidelines on how to build controls into a new automated information system and at the same time show compliance with the directives.

b. There are no formal methods currently in use to easily identify needed controls as systems are being developed. As a result, extensive control reviews are needed after the

system becomes operational. These reviews are costly and may not result in needed corrective actions. To retrofit, the needed adjustments can cost 50 to 100 times more than building the controls into the system as it is being developed.

c. There is no controls process defined that is compatible with, and an integral part of, the total systems process. Rather, there is a tendency to address control issues separate from the many other systems activities.

d. Control and security responsibilities are often assigned to personnel who are organizationally remote from systems development and operation. Although some centralized direction on controls is beneficial, the individuals who understand the requirements and the system must play a major role in the controls development process. To do this, a controls methodology is needed to integrate a controls process into all the many other systems-related activities.

4. Fundamentally, automated information systems are developed to support managers to effectively fulfill their responsibilities. In the Federal Government, automated information systems perform a wide range of functions that include: making benefit payments; collecting receivables; and recording and accounting for obligations, costs, revenues, and expenses. In many cases, these kinds of functions are almost completely dependent on automated information systems, thereby creating many new concerns and risks for management. System risks might, for example, result from the following circumstances:

a. An automated system might allow an individual to circumvent the "separation of duties" control instituted in manual systems.

b. When the information trail is automated (i.e., when all support for payment is in machine form), the "process" may be difficult or impossible to monitor.

c. There is a natural, but totally unfounded, tendency to believe that computer-generated output is correct.

5. To address these concerns, managers who operate or use ADP systems should take actions to eliminate or at least reduce the risks to acceptable levels. All such actions taken to reduce risks are referred to as "control techniques" or, more commonly, "controls." The underlying requirement of control over an automated information system is to provide reasonable assurance that the information processed by the system is reliable and properly safeguarded.

6. Management oversees and effects the development, implementation, and use of automated information systems through a variety of mechanisms, including standards, budget and

procurement review and authorization, and personnel hiring practices. While existing mechanisms have worked with varying success to ensure that systems support an organization's mission, they have not always provided reasonable assurance that a system is safe. Systems may improve accuracy, increase productivity, or speed service but at the same time be subject to fraud, waste, and abuse.

B. SYSTEM CONTROL REQUIREMENTS

1. Control requirements are established to address a known vulnerability or promote reliability or security of a system. They can be based on management experience, vulnerability assessments, other reviews, and/or common sense. Regardless of why established, control requirements should be as specific as possible and stated in clear, understandable terms.

2. Four categories of control requirements surfaced in an analysis of the provisions of the system control directives listed in Table 2-1 on page 2-10. These are application controls, general controls, administrative controls, and required system functions. While the ongoing discussion deals with these four categories of control requirements, it should be recognized here that the operational implementation of a controls program will involve a refining of these requirements into sub-requirements or control objectives.

3. The first category, application controls, are those that help assure that information processed is authorized, valid, complete, accurate, and timely. It also contains requirements that ensure that the system is secure and that an audit trail exists.

4. Compliance with the requirements for application controls has proved the most elusive for management to meet. Requirement terminology varies among the many directives, but the intent is the same in all.

5. Three principles are important to note:

a. How information should be handled, once its sensitivity and/or classification has been determined, is fairly well established by the regulating agency.

b. The determination of the classification levels for systems and data is a management responsibility of the sponsoring agency.

c. Once the classification levels are determined by management, the determinations should be systematically applied, and management should be aware of any exceptions.

FIGURE 2.1 -CONTROL FRAMEWORK

CONTROL REQUIREMENTS

Application Controls
- information authorized
- information valid
- information complete
- information accurate
- information timely
- system secure
- system auditable

General Controls

Administrative controls

Required system functions

SELECTION AND USE OF CONTROL TECHNIQUES

Types of controls
- detective
- corrective
- preventive

Characteristics of effective controls
- have a clear purpose
- developed in partnership
- cost-effective
- documented
- tested and reviewed
- manageable

AREAS OF CONTROL

- input
- output
- processing
- storage
- communications

6. What the third principle means is that sensitive data in a computer data base should have the same classification as they are given in a hard copy publication. Most processes (accounting or otherwise) consist of both manual and automated portions. Reviews of the process should assess the totality of the process components affected, not just a portion of the affected components. Further, management must be aware that increases in security are almost always accompanied by increases in cost, although some security measures can be implemented with little effort. Management must be aware of situations when resources are insufficient to provide the level of protection required, because it is management that must accept the risk of loss and/or disclosure. Because of the terminology and technical complexities of automated processes, the evidence suggests that managers often delegate these critical decisions to their program and/or technical staff. It is of paramount importance that managers fully understand the need for controls, the resource implications of controls, and the risks associated with inadequate controls. These are management's responsibilities and cannot be delegated.

7. The second category, general controls such as cost-benefit analysis and certification, are quantifiable and require a product to be created for management review and/or acceptance. These tools are essential to good management in the development and operation of systems by facility managers, users, systems analysts, and computer programmers. Another essential tool which should be applied by all managers and users is agency record and disposition schedules.

8. The third category, administrative controls such as supportive attitudes or competent personnel, are generally difficult to quantify and have not resulted in the past in tangible work products within automated information systems.

9. Many of the requirements have become standard operation procedures in some Federal Agencies, with considerable guidance provided on how they should be met.

10. The last category of control requirements, required systems functions, consists of mandated features that must be designed and built into a system, such as a particular access capability.

C. SELECTION AND USE OF CONTROL TECHNIQUES

1. Control techniques are procedures used to meet control requirements. Control techniques employed might be preventive, detective, corrective, or a combination of the three:

a. Preventive controls are put in place to prevent or deter any undesired event. Placing a terminal in a locked room,

for example, prevents access to that equipment from personnel without a key.

b. Detective controls are designed to alert management that an undesired event has occurred. An alarm that sounds if the door is forced open, for example, is a detective control.

c. Corrective controls are used in conjunction with detective controls to recover from the consequences of the undesired event. Having insurance to pay for the stolen terminal or a guard force to catch an intruder would be examples of corrective controls.

2. The selection of a control technique should, in most cases, be a group decision to ensure that it is feasible for the entire system, is understood by all affected, and comprehensively meets the organization's control requirements. For example, a user might have to key in special data, operations personnel may have to review exceptions, and a programmer might have to develop codes to be used, because controls can affect many groups associated with the system.

3. Further, the control selected must be cost-effective. (Determining cost-effectiveness for more obvious controls, such as input editing, is usually not an issue.) Controls that require manpower, such as integrity reviews of transactions, can be costly and require a cost-benefit analysis. This analysis becomes part of the controls documentation. Decisions on some controls may also require detailed knowledge of controls already in place. This is especially true of routine controls, such as access controls. The composition of current access controls may greatly affect the design of any additional access controls being contemplated for a particular system.

4. The installation of controls must be accompanied by an effort to provide assurance that the control operates as initially intended. Testing is needed before the control is implemented, as well as later, to be sure it still fulfills the control requirement. Ongoing reviews might be a part of a management initiative. The testing, review schedules and methods are management prerogatives, although external reporting needs would be a consideration. For example, management might decide that test transactions should be reprocessed yearly, while a detailed review of controls documentation should be done each 3 years to coincide with any external reporting requirements specified by OMB Circular A-130 (referenced (e)).

5. The controls selected and implemented must have certain characteristics to ensure that they are effective. They must be:

a. Clear in purpose - If not understood, controls may not be used and if they do not have a clear purpose or address a known vulnerability, they are of little or no value.

b. Coordinated - Developed in partnership by personnel knowledgeable about the application, process, computer systems, and control techniques. It is unlikely that effective, feasible controls can be selected and implemented unilaterally by, for example, a user, a system analyst, a programmer, or an auditor.

c. Cost-effective - The cost of the control should not, in general, exceed the expected benefits. Stated another way, there should be reasonable assurance that the system is protected from a known risk. If total assurance of control were possible, it would probably be prohibitively expensive. More simply, spending $100 to protect against an $80 loss makes little sense.

d. Documented - The documentation process should be simple, understandable, clearly link risks to controls, and provide management with assurance that all reasonable controls are in place. Without some form of documentation, there is no assurance that all known vulnerabilities are addressed or that controls are in place.

e. Tested and reviewed - There must be assurance that the controls function as originally intended. This assurance is needed when the system first becomes operational and also during ongoing operation. Initial controls testing should normally be done when all other aspects of the system are tested. Ongoing testing and review might be done as a part of a general system review, an internal control review, an audit, or other management initiative.

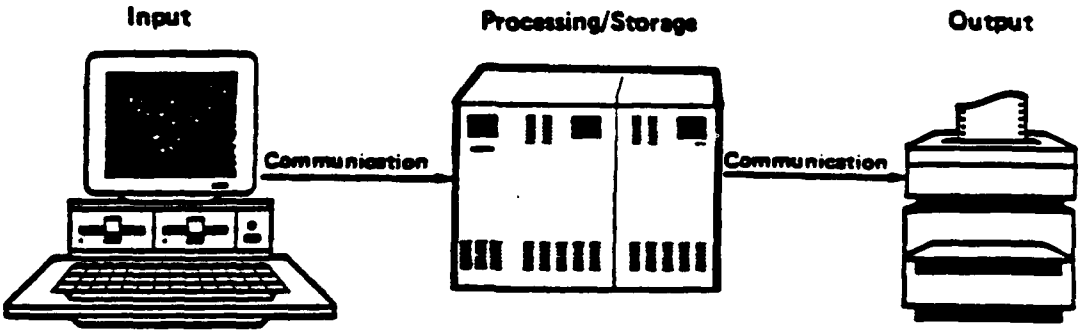
f. Manageable - Management must have the means to change, delete, evaluate cost, upgrade, or review the system of controls under its purview.

D. AREAS OF CONTROL

1. Automated information systems typically encompass data files, computer programs, and equipment, all of which may affect controls in some way. Part of the problem in dealing with controls is the wide variability in how systems are defined. If there was uniformity in definitions, then control techniques could be applied, evaluated, and cataloged more easily.

2. The five control areas listed below are the basic control requirements. These areas, as show in Figure 2-2 on page 2-8, are labeled using traditional terminology.

FIGURE 2-2 - THE FIVE CONTROL AREAS OF A SYSTEM



It is desirable to apply the controls process to one area at a time. This makes the process more manageable, and it also allows similar control issues to be addressed collectively. The control areas are:

a. Input - includes the records (also referred to as either manual data or transactions) to be processed by the system, and the associated processes from origination to the com puter.

b. Output - includes the records and reports produced by the system, and the associated manual processes from the computer to the user.

c. Processing - includes all computer processing to receive the input and store and/or otherwise manipulate the input to produce output.

d. Storage - includes all computer program code and/or instructions and data files.

e. Communications - includes the transmission of data and/or information either between sites or between peripherals at a site.

3. Viewing a system in its pieces makes it easier to set specific control requirements and select control techniques. It is important to retain a system's perspective, to avoid over-control, and to deal with systemwide issues. The following systemwide control issues need to be considered:

a. Control techniques in one control area may lessen the need for controls in another control area; for instance, tight controls over data files may negate the need for some communication controls.

b. Some aspects of a system may require special systemwide attention; e.g., a highly sensitive subfile may require tight controls during inputting, storage, or outputting.

4. This perspective should be the responsibility of individuals or a group that is involved in all aspects of the system. A user group or a controls specialist assigned to the project might be assigned controls responsibility.

5. In general, the framework proposes that control techniques be applied to defined control areas to fulfill control requirements as illustrated in Figure 2-3.

FIGURE 2-3 - MANAGEMENT'S BASIC TASKS IN DEVELOPING SYSTEM CONTROLS

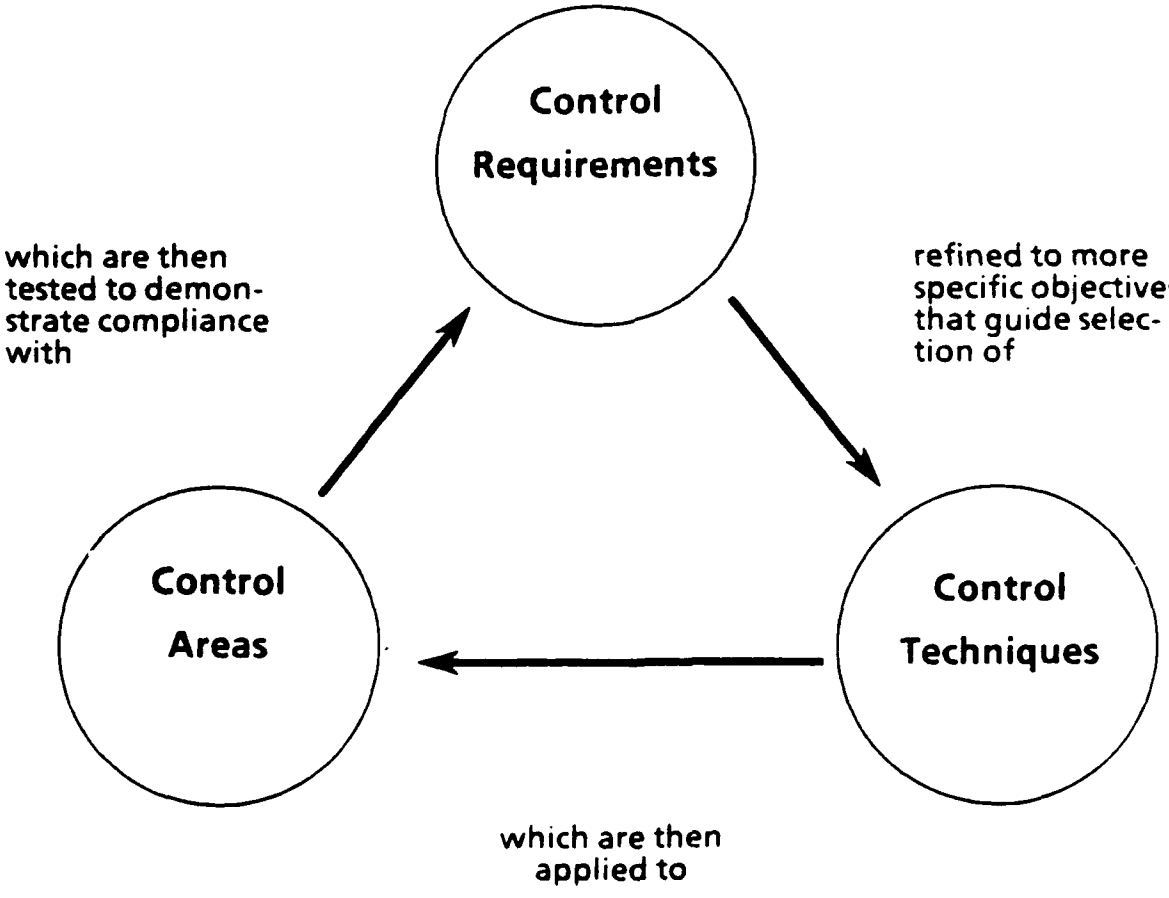


TABLE 2-1 - MAJOR SYSTEM CONTROL DIRECTIVES

DOCUMENT DATE	DOCUMENT TITLE
OMB	
12/82	Office of Management and Budget, Internal Control Guidelines (reference (h))
12/84	Office of Management and Budget, Circular A-127, "Financial Management Systems" (reference (d))
12/85	Office of Management and Budget, Circular A-130, "Management of Federal Information Resources" (reference (e))
8/86 Rev.	Office of Management and Budget, Circular A-123, "Internal Control Systems" (reference (c))
DOD	
6/83	Department of Defense Directive 7740.1,"DoD Information Resources Management Program" (reference (g))
4/87	Department of Defense Directive 5010.38,"Internal Management Control Program" (reference (f))
GAO	
11/84	General Accounting Office, Policy and Procedures Manual for Guidance of Federal Agencies, Title 2 - "Accounting" (reference (i))
10/84	Appendix I, "Accounting Principles and Standards" (reference (j))
10/84	Appendix II, "Standards for Internal Controls in the Federal Government" (reference (k))
PL	
1974	Public Law 93-579,"Privacy Act of 1974," 5 U.S. Code 552a (reference (l))
9/82	Public Law 97-255, "Federal Managers' Financial Integrity Act of 1982," 31 U.S. Code 66a (reference (b))

CHAPTER 3

SYSTEM CONTROL REQUIREMENTS

A. INTRODUCTION

It is through the use of a set of clearly defined objectives that an effective and efficient management controls program is implemented. The requirements constitute a core around which a plan of action can be developed. The 55 control requirements are grouped under the following four categories:

- application controls
- general controls
- administrative controls
- required system functions

B. SYSTEM CONTROL REQUIREMENTS

- APPLICATION CONTROLS

1. Transactions are authorized - the information entered into the system must be authorized by management for entry.

2. Transactions are valid - the information system must process only data that represent legitimate events.

3. Information is complete - all valid data, and only those data, are to be processed by the information system.

4. Information is accurate - data must be free from error during all phases of processing, within defined levels of tolerance.

5. Information is timely - data must reflect the correct cycle, version, or period for the processing being performed. Financial management data shall be recorded as soon as practical after the occurrence of the event, and relevant preliminary data shall be made available promptly to managers after the end of the reporting period.

6. System and data are secure - the data files, computer program, and equipment must be secure from unauthorized and accidental changes, unauthorized disclosure and use, and physical destruction. Detective and corrective controls may also apply depending on the sensitivity and/or classification of the data.

7. System is auditable - an information trail must exist that establishes individual accountability for transactions and permits an analysis of breakdowns in the system and other anomalies.

- GENERAL CONTROLS

8. System controls exist - for each information system, the controls system should ensure that appropriate safeguards are incorporated into the systems, tested before implementation, and tested periodically after implementation.

9. Five-year system plan developed - a plan featuring specific milestones with obligation and outlay estimates for every system of the agency (both current and under development).

10. Contingency plan and/or disaster recovery plan exists - agencies shall develop, maintain, and test disaster recovery and continuity of operations plans for their data center(s). The plan's objective is to provide reasonable continuity of data processing support if normal operations are prevented.

11. Vulnerability assessment conducted - a review of the susceptibility of a program or function to waste, loss, unauthorized use, or misappropriation. Includes both vulnerability assessments or their equivalents, such as an audit.

12. Cost-benefit analysis exists - a review to determine and compare the benefits of the proposed system against the cost of developing and operating the current system. Only those proposals where the expected benefits exceed the estimated costs by 10 percent should be considered for development, unless otherwise specifically required by statute.

13. Reasonable assurance applied - reasonable assurance equates to a satisfactory level of confidence, based on management's judgment of the cost-benefits of the controls versus the recognized risks. (Practically, it is recognized that it is not cost-effective to attain 100 percent assurance.)

14. Control objectives defined - goals established to address a known vulnerability or promote reliability or security of a system.

15. Control techniques selected - methods to satisfy one or more control objectives by preventing, detecting, and/or correcting undesired events. More commonly referred to as "controls."

16. Adequacy of security requirements determined - agencies shall ensure that the appropriate technical, administrative, physical, and personnel security requirements

are included in specifications for the acquisition or operation of facilities, equipment, or software.

17. Security specifications exist - internal control and security objectives must be stated as design specifications and approved by management before development (programming) of the application system can begin.

18. Adequacy of security specifications determined - proof that the design specifications satisfy control objectives must be presented to management to authorize computer program development and/or modification (programming).

19. System design approved - before development (programming) of the system is authorized, management must be assured that the system design satisfies the user's requirements and incorporates the control requirements. The design review must be documented and be available for examination.

20. Controls documented - internal control systems, including all transactions and significant events, are to be clearly documented and be readily available for examination.

21. System documentation exists - documentation that must reflect the current state of the system as it is being operated. The documentation must be sufficient to ensure effective operation by users and system maintenance by programmers.

22. System contingency plan exists - plans must be developed, documented, and tested to ensure that users of the system can continue to perform essential functions in the event their information technology support is interrupted. The plan should also be consistent with the agencywide disaster recovery plan.

23. Controls tested - before a new or modified system is placed into production status, the controls should be tested to prove that the controls operate as intended. The test results should be documented and sent to management for approval to implement the system.

24. System test conducted - before implementation of the system is authorized, evidence that the system operates as intended must be presented to management. This evidence must also include the results of controls testing. The test results must be documented and available for examination.

25. Test results documented - the documentation should demonstrate that the control and functionality requirements operate as intended.

26. System certified prior to implementation - before a system can be implemented, an agency official shall certify that

the system meets all applicable Federal policies, regulations, and standards, as well as state that test results demonstrate that installed controls are adequate for examination.

27. Controls review performed - periodically, the controls of each system must be tested to determine if the controls still function as intended. The results of these tests must be documented and available for examination.

28. Periodic reviews and recertifications are conducted at least every 3 years, agencies shall review applications and recertify the adequacy of the safeguards. The recertifications shall be documented and be available for review.

29. Periodic risk assessments are conducted - agencies shall conduct periodic risk assessments at each data center to provide a measure of the relative vulnerabilities and threats to the data center so that security resources can be effectively distributed to minimize potential loss.

30. Corrective action taken; audit findings resolved promptly - managers are to promptly evaluate audit findings and recommendations, determine proper corrective actions, and complete those actions.

31. Annual report on internal controls prepared - yearly, each agency must determine if its systems of internal controls are in compliance with the Comptroller General's standards.

32. Annual report on accounting systems prepared - yearly, each agency must determine if its accounting systems are in compliance with the Comptroller General's standards.

33. Annual reports to President sent - the head of each agency must sign both annual reports and transmit them to both the President and Congress.

- ADMINISTRATIVE CONTROLS

34. Organizational responsibility is affixed - the assignment of responsibilities for planning, directing and controlling the controls evaluation process for the agency and/or segment is specified. The programs and functions conducted in each of the components have also been specified.

35. Separation of duties exists - key duties and responsibilities in authorizing, processing, recording, and reviewing transactions should be separated among individuals.

36. Supervision is provided - qualified and continuous supervision is to be provided to ensure that control requirements are met.

37. Supportive attitudes exist - managers and employees are to maintain and demonstrate a positive and supportive attitude toward controls at all times.

38. Personnel are competent - managers and employees are to have personal and professional integrity and are to maintain a level of competence that allow them to accomplish their assigned duties, as well as understand the importance of developing and implementing good controls.

39. Security training program exists - agencies shall establish a security awareness and training program so that agency and contractor personnel involved with information systems are aware of their security responsibilities and know how to fulfill them.

40. Written policies and procedures exist - each agency shall establish administrative procedures to enforce the intended functioning of controls, including provisions that performance appraisals reflect execution of control-related responsibilities.

41. Personnel security policies exist - each agency should establish and manage personnel security procedures, including requirements for screening agency and contractor personnel designing, developing, operating, maintaining, or using the system. The level of screening depends on the sensitivity and/or classification of the system data.

42. Individual responsibilities are affixed - assignments of responsibility should be made for internal controls, accounting systems, and data center security on an agencywide and individual system and/or center basis.

43. Custody and/or accountability assigned - the official whose function is supported by an information system is responsible and accountable for the products of the information system.

44. Record disposition procedures exist - each agency must establish approved records disposition schedules which identify permanent data files and ensure their transfer to the National Archives and Record Administration.

45. Release of information provided for - each agency must have procedures in place so that information can be extracted from systems to meet requests made under the Privacy Act and the Freedom of Information Act.

- <u>REQUIRED SYSTEM FUNCTIONS</u>

46. An analysis of the ratio of outputs to inputs evaluated against an acceptable standard.

47. System operation is economical - uneconomical systems must be identified and phased out.

48. System is effective - periodically, each system should be reviewed to determine if the system still meets organizational needs.

49. System supports management - data shall be recorded and reported in a manner to facilitate carrying out the responsibilities of both program and administrative managers.

50. System supports budget - financial management data shall be recorded, stored, and reported to facilitate budget preparation, analysis, and execution.

51. Comparability and/or consistency provided for - financial management data shall be recorded and reported in the same manner throughout the agency, using uniform definitions that are synchronized with budgeting and used consistently for each reporting period.

52. Information is useful and/or relevant - data capture and reports shall be tailored to specific user needs, and if usage does not justify costs, data or reports shall be terminated.

53. System provides full disclosure - data shall be recorded and reported to provide users of the data with complete information about the subject of the report per OMB, Treasury, and Privacy Act standards.

54. Individual access allowed - systems must be able to extract any data contained in the data base about individuals to meet requests to see the data by that individual or his/her representative when required by the Privacy Act.

55. Network compatibility exists - any systems developed or acquired must be interoperable with any existing system that will be linked to the new system.

C. CROSS-REFERENCE TO CONTROL DIRECTIVES

Table 3-1 on page 3-7 provides a listing of the 55 control requirements cross-referenced to the major control directives cited in Chapter 2.

Table 3.1 Summary table of control objectives cross-referenced to the major control directives.

Line No.	Requirements	A-123	OMB IC	A-127	A-130	GAO Title II	FMFIA	Privacy Act	DoD IMCP	DoD IRMP
	Application Controls									
1.	Transactions are authorized	X	X		X	X		X		
2.	Transactions are valid	X	X		X	X	X			
3.	Information is complete	X	X	X		X	X	X		X
4.	Information is accurate	X	X	X	X	X	X	X		X
5.	Information is timely	X	X	X		X	X	X		X
6.	System and data are secure				X		X	X		X
7.	System is auditable			X		X				
	General Controls									
8.	System controls exist				X	X				
9.	5-year system plan developed			X	X	X			X	
10.	Contingency plan/organization disaster recovery plan exists				X	X				X
11.	Vulnerability assessment conducted	X	X			X			X	
12.	Cost/benefit analysis exists					X				X
13.	Reasonable assurance applied	X	X	X	X	X	X		X	
14.	Control objectives defined	X	X			X			X	
15.	Control techniques selected	X	X			X			X	
16.	Adequacy of security requirements determined				X					
17.	Security specifications exist				X	X				X
18.	Adequacy of security specifications determined				X					
19.	System design approved				X	X				
20.	Controls documented	X	X			X				
21.	System documentation exists					X				
22.	System contingency plan exists				X	X				
23.	Controls tested				X	X				
24.	System test conducted					X				
25.	Test results documented				X	X				
26.	System certified prior to implementation				X					
27.	Controls review performed	X	X	X		X	X			
28.	Periodic reviews and recertifications are conducted			X	X	X			X	X

Table 3.1 Continued-Summary table of control objectives cross-referenced to the major control directives.

29. Periodic risk assessments are conducted				X	X			X	
30. Corrective action taken; audit findings resolved promptly	X	X			X			X	
31. Annual report on internal controls prepared			X	X		X		X	
32. Annual report on accounting systems prepared					X	X		X	
33. Annual reports sent to President	X	X		X	X	X		X	
Administrative Controls									
34. Organizational responsibility is affixed		X						X	X
35. Separation of duties exist	X	X			X			X	
36. Supervision is provided	X	X			X			X	
37. Supportive attitudes exist	X	X			X			X	
38. Personnel are competent	X	X			X			X	
39. Security training program exists				X				X	
40. Written policies and procedures exist	X	X	X					X	X
41. Personnel security policies exists				X				X	
42. Individual responsibilites are affixed	X	X	X	X	X			X	
43. Custody/accountability assigned	X	X		X	X	X		X	X
44. Record retention procedures exist							X		X
45. Release of information is provided for							X	X	X
Required System Functions									
46. System is efficient			X		X				X
47. System operation is economical			X		X				
48. System is effective				X	X				X
49. System supports management			X					X	X
50. System supports budget			X		X			X	
51. Comparability/consistency provided for			X		X				
52. Information is useful/relevant			X	X	X		X		X
53. System provides full disclosure			X		X		X		
54. Individual access allowed				X		X	X		
55. Network compatibility exists				X					

CHAPTER 4

INTERNAL CONTROL THROUGH LIFE-CYCLE MANAGEMENT DOCUMENTATION

A. INTRODUCTION

One method of establishing good internal controls is to use the documentation produced throughout the life-cycle of an Automated Information System (AIS). These documents are described in DoD 7935.1-STD, DoD Directive 7920.1, and DoD Instruction 7920.2 (references (m), (n), and (o)). Appendix A has been included to show the internal control techniques that need to be considered during the documentation of AIS tasks. Life-Cycle Management (LCM) provides an LCM review and milestone approval structure that identifies key decision points during the time from system inception to system termination or replacement.

B. BACKGROUND

1. LCM is a control process applied to expenditures on AISs and for administering an AIS. It emphasizes early decisions that shape AIS costs and utility and are based on full consideration of functional, hardware, software, and telecommunications requirements. The life-cycle of an AIS is composed of six broad phases: Need Justification; Concepts Development; Design; Development; Deployment; and Operations. (See Table 4-1 page 4-5).

2. LCM seeks to achieve the following objectives:

a. Control expenditures on AISs to ensure that the benefits derived from an AIS are responsive to user needs and accomplished in the most cost-effective manner.

b. Provide a management structure for AIS developments.

c. Establish a standard management discipline to ensure that an AIS is developed, evaluated, and operated at the lowest total overall cost.

d. Provide early visibility of all resource requirements.

e. Promote standardization, and AIS interoperability wherever appropriate.

C. LIFE-CYCLE PHASES

1. Need Justification Phase (Phase 0). The purpose of this phase is to identify a mission need, validate that need, and recommend the exploration of alternative functional concepts to satisfy the need.

a. Documentation during this phase should address the following concerns such as:

(1) Quantifying the mission deficiencies and goals for improvement.

(2) Characterizing the current and projected environment to include wartime role, if any.

(3) Estimating overall costs to include time and level of effort.

(4) Determining affordability constraints.

(5) Clarifying and focusing the mission needs.

(6) Determining what needs can be satisfied using current capabilities.

(7) Establishing need priorities.

(8) Determining the timing and urgency of the needs.

(9) Security and other vulnerabilities.

b. Documentation produced during this phase. Mission Need Statement (MNS)*, which takes into account considerations such as Mission Area Identification, and Deficiencies. [*Note: A Mission Need Statement will be prepared for each major AIS in accordance with reference (n)]

2. Concepts Development (Phase 1). The purpose of this phase is to identify and evaluate alternative methods to satisfy the mission need, and to select the best program to implement the required capabilities.

a. Documentation during this phase should address the following concerns:

(1) Defining alternate functional architectural concepts.

(2) Weighing the risks of each workable concept.

(3) Selecting a concept based upon an adequate feasibility analysis.

(4) Developing demonstrations for each alternate functional concept, if required.

(5) Conducting a cost-benefit analysis.

(6) Determining an initial cost estimate.

(7) Establishing a configuration management discipline.

(8) Developing an acquisition strategy.

b. Documentation produced during this phase:

(1) Project Management Plan.

(2) Functional Description.

(3) Acquisition Plan.

(4) Cost-Benefits Analysis.

(5) Resources Document.

(6) Preliminary plans adequately describe a concept for training, logistical support, organizational relationships and, if appropriate, operation of an automated system.

(7) System Decision Paper 1 *. [*Note: A System Decision Paper (SDP) will be prepared for each major AIS in accordance with reference (o)]

3. Design (Phase 2). The purpose of this phase is to complete the AIS technical specifications, and validate the selected system design.

a. Documentation during this phase should address the following concerns:

(1) Revalidate mission needs.

(2) Weigh the risks of each alternate design.

(3) Validate AIS and/or Telecommunications adequacy.

(4) Select the best design.

(5) Complete the economic analysis.

(6) Obtain design approvals from functional proponent and technical managers.

(7) Develop a firm baseline for requirements, costs, and schedules.

(8) Plan for new facilities.

(9) Provide for full funding of the program.

b. Documentation produced during this phase:

(1) Data Requirements Document.

(2) Program Specifications.

(3) Data Base Specifications.

(4) System and/or Subsystem Specifications.

(5) Configuration Management Plan.

(6) Economic Analysis.

(7) Plans for training, logistics support, telecommunications, security, integration, and operations have been developed and updated.

(8) *System Decision Paper 2 *.* [*Note: A System Decision Paper (SDP) will be prepared for each major AIS in accordance with reference (o)].

4. Development (Phase 3). The purpose of this phase is to develop the total AIS, test the completed AIS to ensure that it satisfies missions needs, and prepare for deployment.

a. Documentation during this phase should address the following concerns:

(1) Completion of the development of the system.

(2) Completion of operational testing and evaluation.

(3) Implementation planning.

(4) Current risk assessment and future risk management actions.

(5) Current requirements, costs, and schedule baselines.

(6) Full funding of the program.

b. Documentation produced during this phase:

(1) Computer programs and data bases.

(2) Users Manual.

(3) Computer Operations Manual.

(4) AIS Security Certification and/or Accreditation.

(5) Deployment and Operations Plans.

(6) Continuity of Operations Plan.

(7) Logistics Support and Training Plans.

(8) Test and Evaluation Plan.

(9) Functional and Physical Configuration Review.

(10) Test Analysis Report.

(11) System Decision Paper 3 *. [*Note: A System Decision Paper (SDP) will be prepared for each major AIS in accordance with (reference (o)].

5. Deployment (Phase 4) and Operations (Phase 5). The purpose of these phases are to: (1) field the AIS in accordance with the approved deployment plan; and (2) operate and maintain the AIS, evaluate its effectiveness, and plan for long-term AIS modernization.

a. Documentation should address the following concerns:

(1) Security procedures.

(2) System reviews and audits.

(3) Formal change control process.

(4) Deployment and Operation schedules.

6. Documentation produced during these phases. Implementation Procedures.

a. Deployment Phase.

(1) Updated SDP.

(2) Updated Baseline Document.

b. Operations Phase.

(1) Updated SDP.

(2) updated Baseline Document.

(3) Existing AIS Modernization Plans.

TABLE 4.1 - LIFE-CYCLE MANAGEMENT PHASES - MILESTONES - DOCUMENTATION

MILESTONES	0	I	II	III	IV	V
	NEED JUSTIFICATION Phase 0	CONCEPTS DEVELOPMENT Phase 1	DESIGN Phase 2	DESIGN Phase 3	DEPLOYMENT Phase 4	OPERATION Phase 5
			Define / Design	Define / Design		
SDP DOCUMENTATION						
	MNS	ES PMP RES ASP SUP	TEP			

MNS - Mission Need Statement
ES - Executive Summary
PMP - Project Management Plan
RES - Resource Document

ASP - Acquisition Strategy Plan
SUP - Support Plans
TEP - Test and Evaluation Plan

SDP DOCUMENTATION						
	FD	RD	SS PS DS	UM OM MM PT	RT	IP

FD - Functional Description
RD - Data Requirements Document
SS System/Subsystem Specification

PS - Program Specification
DS - Data Base Specification
UM - Users Manual

OM - Computer Operation Manual
MM - Program Maintenance Manual
PT - Test Plan

RT - Test Analysis Report
IP - Implementation Procedures

CHAPTER 5

RISK ASSESSMENTS

A. INTRODUCTION

1. The purpose of this chapter is to provide DoD managers guidance on assessing risks in automated information systems. While introducing efficiencies in governmental activities, automation simultaneously introduces new and different vulnerabilities. A risk assessment is conducted to determine susceptibility to waste, loss, and abuse.

2. Based on the results of risk assessment, an agency can proceed with its internal control evaluation, improvement and reporting process.

3. Under revised OMB Circular A-123, (reference (c)), agencies are required to make risk assessments to identify potential risks in agency operations that require corrective action or further investigation through internal control evaluations or other actions. These may follow the risk assessment procedures in the Internal Control Guidelines or may be based on a systematic review building on management's knowledge, information obtained from management reporting systems, previous risk assessments, audits, etc. Management should update its risk assessment of components at least once every 5 years and as major changes occur.

4. OMB Circular A-130, (references (e)) requires agencies to establish a level of security for information systems commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the information systems.

B. BASIC APPROACH

1. Internal controls should provide reasonable, although not necessarily absolute, assurance of minimal risks. Reasonable assurance recognizes that the costs of developing and instituting internal controls should not exceed the benefits derived from reducing risks. Risk assessment consists of four measures:

a. Analyzing the management control environment.

b. Evaluating general automated system controls.

c. Evaluating application controls.

d. Evaluating inherent risks associated with programs or functions supported by automated systems.

2. Questionnaires were developed to help managers gather and analyze information about the system's internal controls. The questionnaires are self-explanatory. Responses will be a simple "yes" or "no." Several "no" responses within one section may indicate control weaknesses, and depending on inherent risk, may indicate high vulnerability. However, judgment needs to be applied. For example, one "no" response to a critical question could indicate the need for a more detailed internal control review and the need for corrective action.

C. QUESTIONNAIRE 1 - ANALYSIS OF THE MANAGEMENT CONTROL ENVIRONMENT. Questionnaire 1 has been developed to assist in analyzing the management control environment in which automated operations or applications are conducted. First, management must assess the potential for waste, loss, mismanagement, unauthorized use, or misappropriation that exists in each automated operation or application. Second, management's control systems must be examined. To assess the management control environment, several factors should be considered, including:

- AIS Standards, Policies, and Procedures
- AIS Planning, Budgeting, and Reporting
- Prior Internal Audits and Reviews, and Management's Responsiveness
- AIS Quality Assurance

1. AIS Standards, Policies, and Procedures Considerations: Implementing IRM policies and procedures should cite and be based on authorizing legislation, Departmental regulations, and Federal regulations concerning IRM, as appropriate. They should be updated to remain current. These policies and procedures must be promptly distributed to those who have internal control responsibilities and should include specific control guidance for AIS activities. "YES" answers to the following questions would indicate a low vulner-ability to risk.

	YES	NO
a. Has management initiated policies and proce-dures for timely implementation of DoDIRM standards?	___	___
b. Are changes to existing policies and procedures disseminated promptly to all appropriate organizational units and individuals?	___	___

	YES	NO
c. Have internal control and security objectives been defined in regard to automated operations and applications?	___	___
d. Are specific internal controls, resource acquisition, system development and modification, and operating policies and procedures issued under these DoD standards?	___	___

2. IRM Planning, Budgeting, and Reporting Considerations. Management's commitment to meeting goals concerning planning, budgeting, and reporting practices should reflect current Government policy and be widely publicized. Goals should include: (1) establishing budgeting policies; (2) adherence to these policies; and (3) development and use of short- and long-range planning. "YES" answers to these questions reflect a low vulnerability to risk in this area.

	YES	NO
a. Does an Advisory Council exist, meet regularly, and is it chaired by a top management representative?	___	___
b. Does the planning process include short- and long-range plans and clearly establish and document mission requirements, strategy, goals, and objectives?	___	___
c. Does the planning process consider budgeting for financial, personnel, technical resources (e.g., hardware, software, communications and system interface) and compare and select among alternatives based upon quantified life-cycle costs, benefits and risk projections?	___	___
d. Are plans usually followed? If not, are deviations from plans adequately documented with justification?	___	___
e. Are plans and budgets for financial, personnel, and technical resources consistent with Departmental plans and budgets?	___	___

3. Considerations Concerning Prior Internal Audits and Reviews and Management's Responsiveness. The assessment of an AIS vulnerability may be supported by reviews or audits by Internal Audit (the Inspector General where that organization exists), the U.S. General Accounting Office, or congressional committees. The primary considerations in this area are the corrective actions identified and management's response to them. "YES" responses to the following questions indicate low vulnerability.

	YES	NO
a. Does the Internal Audit function perform audits of operational systems, systems under development, and other activities addressing general and application controls?	___	___
b. Are corrective actions identified as a result of audits or reviews of the automated operation or application?	___	___
c. Are there no significant audit or review findings that represent continuance of previously identified problems?	___	___

4. AIS Quality Assurance Considerations. Quality assurance is a critical function in the automated information systems environment to ensure user departments are satisfied with the quality of information systems. Quality assurance should be responsible for reviewing all aspects of information systems to ensure adherence to the standards and implementing policies and procedures. In addition, the quality assurance function should be responsible for ensuring the accuracy and reliability of automated systems' outputs. "YES" answers to the following questions indicate low vulnerability to risk in the area.

	YES	NO
a. Has a quality assurance function been established to determine if user departments are satisfied with the quality of automated systems and tested internal controls incorporated in the information systems?	___	___
b. Is the quality assurance function responsible for reviewing all aspects of automated systems to ensure adherence to standards, policies and procedures?	___	___

	YES	NO
c. Does the quality assurance function monitor the accuracy and reliability of automated systems' outputs?	___	___

D. QUESTIONNAIRE 2 - EVALUATION OF GENERAL SYSTEMS CONTROLS. This questionnaire helps to determine if general systems controls are in place to prevent or minimize waste, loss, mismanagement, unauthorized use, or misappropriation. The level of comprehensiveness and intensity of review depends on the size of the system, including hardware and software. This questionnaire focuses on the following aspects of automated general control:

- Organizational Checks and Balances.
- Data Center Operations.
- Security and Control.
- Environmental Protection and Disaster Recovery and/or Contingency Planning.
- System Design, Development, and Modification Control.
- System Software Control.
- Distributed Processing and Network Operations Control.
- Personnel.
- Microcomputer Control.

1. Organizational Checks and Balances Considerations. Effective internal controls need to be established over the data processing operations and applications because of the concentration of functions brought about by the computer. "YES" responses to the following questions indicate low vulnerability to risk in this area.

	YES	NO
a. Are duties separated to ensure no individual performs more than one of the following functions;		
(1) Originating Data.	___	___
(2) Processing Data.	___	___
(3) Distributing Data.	___	___
(4) Inputting Data.	___	___

	YES	NO
(5) Reviewing Data.	___	___
b. Are duties separated among computer operations, systems development, systems programming, applications programming, and data control?	___	___
c. Are duties and separation requirements documented and enforced?	___	___

2. Data Center Operations Considerations: Control procedures for data center operations should be established and followed to ensure accuracy and completeness of the information maintained and processed by the DoD data centers. "YES" responses to the following questions indicate low vulnerability to risk in this area.

	YES	NO
a. Does a formal production schedule exist to ensure that resources are effectively used and that the needs of users are met?	___	___
b. Is a formal control group established within the data center to monitor both decentralized and centralized job entry?	___	___
c. Does a schedule exist for preventive maintenance according to established site and vendor procedures?	___	___
d. Are formal malfunction reporting procedures established, documented, and enforced?	___	___
e. Are procedures for user billing and charge-back documented and are such procedures tied into a job accounting system for the data center's resources?	___	___
f. Do detailed written operator instructions (including set-up, file disposition, error response and restart and/or recovery) exist and are they followed?	___	___

	YES	NO
g. Are supervision and review of operations sufficient to provide reasonable assurance that the computer is used only for authorized purposes and that operators are following prescribed procedures?	___	___

3. Security and Control Considerations: Control and/or procedures consistent with DoDD Directive 5200.28 and OMB Circular A-130 references (r) and (e)), for computer security should be established and followed to safeguard ADP resources. The hardware, software, and data are all assets that should be protected against theft, loss, unauthorized manipulation, fraudulent activities, and natural disasters. To minimize these risks, controls to limit access to the data center, decentralized hardware including microcomputers, system and application programs, system documentation and output should be established. "YES" responses to the following questions indicate low vulnerability to risk in this area.

	YES	NO
a. Is responsibility for computer security at the site established, documented, and assigned?	___	___
b. Are required controls in place to protect national security information?	___	___
c. Are clearly defined security policies and procedures established and enforced?	___	___
d. Are risk analyses performed according to a specific timetable?	___	___
e. Are personnel security policies for screening employees and contractor and/or service personnel documented and enforced?	___	___
f. Is access to the computer area by individuals in need of limited access (e.g., hardware manufacturer, custodial personnel, etc.) supervised and controlled?	___	___
g. Are procedures limiting access to critical forms, such as identification cards, checks, and source documents, documented and enforced?	___	___

	YES	NO
h. Are user identification codes and passwords used to validate users of the system, data and software?	___	___
i. (1) Is separate computer access control and/or security software utilized?	___	___
(2) Does it control access to individual data files and elements, application programs, and other system software?	___	___
(3) Are accesses to the system recorded (either manually or automatically)?	___	___

4. Environmental Protection and Disaster Recovery and/or Contingency Planning Considerations: Procedures should be established to help protect critical files, programs, and system documentation from fire or other natural disasters. These procedures should be formally documented and periodically updated and tested. They should contain the detailed steps computer operations personnel should take in the event of an emergency. The data center should be equipped with both smoke and fire detection devices. Floors, walls, ceilings, and draperies should be made of noncombustible material. Alternate power sources or other electrical backup devices should be installed to limit the impact of a power shortage or blackout. Formal backup arrangements should also be established with another compatible data center. Copies of critical files, programs, and documentation should be stored at an off-site location. Steps should be taken to make sure that the off-site materials are periodically updated and that the backup center has sufficient capacity to process the additional work load. Periodic tests of the backup arrangements should also be performed.

	YES	NO
a. Have emergency disaster recovery and/or contingency planning procedures been documented and are they up-to-date?	___	___
b. Do they include steps to take in the event of a natural disaster by fire, water damage, etc., and intentional damage by sabotage, mob action, bomb threats, etc?	___	___
c. Are employees familiar with the emergency procedures?	___	___

		YES	NO
d	Is the data center separated from adjacent areas by fire resistant partitions, walls, etc.?	___	___
e.	Are noncombustible floors, ceiling, and/or draperies used in the data center?	___	___
f.	Are any activities conducted adjacent to the data center that might endanger it by flood, fire, or explosion?	___	___
g.	Are heat and smoke detectors installed in the following areas:		
	- In the ceiling?	___	___
	- Under raised floors?	___	___
	- In the air return ducts?	___	___
h.	Are battery-powered emergency lights placed in strategic locations to assist in evacuation should power be interrupted?	___	___
i.	Is the data center protected by an automatic fire-suppressing system?	___	___
j.	Is the data center equipped with temperature and humidity gauges that automatically acti-vate signals if either exceeds the normal range?	___	___
k.	Is the data center backed up by an uninterruptable power source system?	___	___
l.	Are there provisions for retaining and/or copying master files and a practical means of reconstructing a damaged or destroyed file?	___	___
m.	Are sufficient generations of files maintained to facilitate reconstruction of records?	___	___
n.	Are duplicate copies of data files application programs, system software, and critical documentation kept and updated periodically ata remote location and restricted from unauthorized access?	___	___

	YES	NO
o. Is there backup capability at an off-site location?	___	___
p. Have critical locations been provided with adequate terminals, modems, and communications lines?	___	___
q. Are operations procedures periodically tested at the backup data center?	___	___

5. Application Design, Development, and Modification Control Considerations. Systems design, development, and modification process should provide adequate separation of duties and assure user, management, and internal audit participation. Additional key elements are documentation, computer program testing, system acceptance testing, and computer program change control procedures. The age and life expectancy of an application or operation will determine to some degree its susceptibility to fraud, waste, loss, unauthorized use, or misappropriation. "YES" responses to the following questions indicate low vulnerability to risk in this area.

	YES	NO
a. Is the application development predicated on a system development life-cycle methodology?	___	___
b. Are formal, standard control practices followed in system design and development and are they reviewed for proper implementation?	___	___
c. Are systems documented as they are being designed?	___	___
d. Are new or modified programs and/or systemssubjected to comprehensive testing (both computer program and user acceptance) prior to implementation?	___	___
e. Are test results approved by user departments and AIS management prior to conversion to a new system?	___	___
f. Are system development, pre-implementation and post-implementation reviews of an entire (manual and automated) system performed?	___	___

	YES	NO
g. Are procedures in place that define who can initiate a system change request and who can authorize a change?	___	___
h. Is a log kept of completed system changes and changes in process?	___	___
i. Is the application or operation using up-to-date techniques and being maintained by people familiar with the techniques?	___	___
j. Is the application stable or undergoing only minor or well-controlled enhancements?	___	___

6. Systems Software Control Considerations. System software purchased from vendors is normally reliable and includes built-in error checking features capable of detecting any processing errors it might cause. However, through program changes and software options, systems software support personnel control many details of computer operations and application processing. "YES" responses to the following question indicate low vulnerability in this area.

	YES	NO
a. Are modifications to system software authorized and approved by ADP management before changes are made?	___	___
b. Is access to system software and related documentation restricted to authorized personnel?	___	___
c. Are procedures established, documented and enforced to provide assurance that systems software changes are thoroughly and independently tested and properly implemented?	___	___

7. Distributed Processing and Network Operations Control Considerations. Control procedures for distributed processing and network operations should be formally established and followed. With the rapid increase of decentralization of systems, control and integrity have become major concerns. "YES" answers the following questions indicate low vulnerability in this area.

	YES	NO
a. Are standards and policies for general network control clearly established and followed?	___	___
b. Does a network policy exist requiring audit trails and backup of all network communications activity for both network messages and applications-processed data?	___	___
c. Do distributed processing and network hardware controls include memory protection, alternate communications routing, communication protocols and timely failure and/or recovery mechanisms?	___	___
d. Are local and consolidated network p erformance reports prepared to regularly convey key elements, such as network s ystems availability, performance to schedules, response times, processing efficiencies, and performance problems?	___	___
e. Are local and/or private communications lines and switches secured and accessible only by authorized personnel?	___	___
f. Are communications security methods used toprotect transmission of sensitive and/ornational security information?	___	___

8. Personnel Considerations. Important factors in this area are the integrity and competency of contractor and agency personnel assignedto carry out AIS operations and applications activities. Personnel must have adequate experience and training to be competent. "YES" answers to the following questions indicate low vulnerability to risk in this area.

	YES	NO
(1) Are appropriate security clearances granted prior to allowing personnel access to sensitive or national security information?	___	___
(2) Do key personnel receive adequate training in the professional, technical, internal control and security aspect of their jobs?	___	___

	YES	NO
(3) Are employees regularly informed of new policies and procedures including internal management control requirements?	___	___

9. Specific Microcomputer Control Considerations. Control procedures for microcomputer operations should be established and followed to ensure the proper management and use of microcomputers and the accuracy of the processed data. Implementing certain control procedures unique to microcomputers should decrease the risk of illegal system access, data loss, and stolen hardware. "YES" responses to the following questions indicate low vulnerability to risk in this area.

	YES	NO
a. (1)Have policies and procedures regarding the acquisition and use of microcomputer resources been developed?	___	___
(2)Are policies regarding the acquisition and use of microcomputer resources adhered to and enforced?	___	___
(3)Do policies prohibit the use of copyrighted and/or unauthorized software that the activity has not leased or purchased?	___	___
b. Are the functions and capabilities of microcomputer based systems documented?	___	___
c. Are microcomputer resources inventories, hardware and software, maintained in a central location and verified periodically?	___	___
d. Do adequate controls exist to ensure that microcomputer hardware is not stolen or vandalized?	___	___
e. Are guidelines followed for the backup of programs and files, and for their safe-keeping?	___	___
f. Are labeling and storage procedures for sensitive information, storage media and microcomputers established?	___	___

E. QUESTIONNAIRE 3 - EVALUATION OF APPLICATION CONTROLS

This questionnaire helps to determine if appropriate application controls are in place. Users of automated information systems have primary responsibility for assuring their systems have adequate controls, including security. Users should establish the sensitivity or the risk and magnitude of loss or harm that could result from improper operation of their application. Appropriate administrative, physical, and technical controls should be implemented by users. This questionnaire is intended to be used when reviewing functional controls of agency activities that use ADP to support their activities. It focuses on the following aspects of automated application control:

- Purpose and Characteristics.
- Assuming the Risk at the Data Center.
- Data Origination.
- Data Input.
- Data Processing.
- Data Output.

1. Purpose and Characteristics Considerations: The purpose and characteristics of the ADP application should be evaluated by its user to determine the degree to which it is susceptible to waste, loss, unauthorized use, mismanagement, or misappropriation. For example, ADP applications that maintain or process classified or sensitive data that may (1) have a significant impact outside the department or agency; (2) cause transfers of property or receipt and/or payment of money; or (3) involve approvals or granting of authority that are sensitive and, thus, particularly vulnerable. "YES" answers to the following questions indicate low vulnerability.

	YES	NO
a. Have the users made a clear determination of the sensitivity of each application and the information processed?	___	___
b. Is that determination based on the total risk and magnitude of loss or harm that could result from improper operation of the application or disclosure of information?	___	___

	YES	NO
c. Where the application is considered sensitive, has the user:		
(1) Participated in defining and approving security specifications for the application?	___	___
(2) Verified that security controls are working and have been certified as operationally adequate for the application?	___	___
(3) Reviewed and recertified the application in the last 3 years?	___	___
(4) Assured that security or other control weaknesses have been corrected?	___	___
(5) Included security or other control weaknesses found in their annual report?	___	___
(6) Assured that procedures are in place that control who can initiate a change and who can authorize a change?	___	___

2. Assuming the Risk at the Data Center: Since users of ADP have ultimate responsibility for the security and integrity of their application, they assume the level of risk at the installation that processes their application. It is critical, therefore, that they have the ability to reduce that risk to an acceptable level (even if required to go to a different installation for processing). "YES" responses to the following questions indicate low vulnerability in this area.

	YES	NO
a. Does the user organization understand the level of risk at the installation where his or her application is processed?	___	___
b. Is the user organization apprised of changes at the installation that may impact that level of risk?	___	___
c. Does the user understand the vulnerability of the communication lines and links used in the application?	___	___

	YES	NO
d. Does the user know who is responsible for security at the installation where his or her application is processed?	___	___
e. Is the user organization free to seek data processing support at a different installation?	___	___
f. Is the user familiar with the disaster recovery and backup plan at the data processing installation where his or her application is processed?	___	___
g. Does the user have a contingency plan consistent with the disaster recovery and backup plan for essential functions?	___	___
h. If a data base management system is used in the users' application, does he or she understand its vulnerabilities and special control considerations?	___	___
i. Does the user have secutity measures in placeto protect ADP equipment, such as microcomputers and remote terminals in his or her area?	___	___

3. Data Origination Considerations: Data origination controls are used to ensure the accuracy, completeness, and timeliness of data prior to its being converted into a machine-readable format and entered into the computer application. Controls should ensure that the data reaches the computer application without loss, unauthorized addition, modification, or error. "YES" responses to the following questions indicate low vulnerability to risk in this area.

	YES	NO
a. Do documented procedures exist to explain methods for proper source document origination, authorization, data collection, input preparation, error handling, and retention?	___	___
b. Are duties appropriately segmented for originating data, inputting data, processing data, distributing output, and reviewing output?	___	___
c. Are signatures required to approve all transactions?	___	___

	YES	NO
d. Are source documents accounted for?	___	___
e. Is access to source documents, blank input forms, and copies of source documents restricted only to authorized personnel?	___	___
f. Do documented procedures exist to explain the methods for source document error detection, correction, and reentry?	___	___

4. Data Input considerations: Data input controls ensure the accuracy, completeness, and timeliness of data during its conversion into machine-readable form and entry into the application. Data can be input through either on-line or batch processing. "YES" responses to the following questions indicate low vulnerability to risk in this area.

	YES	NO
a. Are procedures established for the conversionand entry of data to ensure separation of duties as well as routine verification of work performed in the data input process?	___	___
b. Are procedures related to the conversion and entry of data through terminals, such as the use of passwords, followed to deter unauthorized use?	___	___
c. Do documented procedures exist to explain the process of identifying, correcting, and reprocessing data rejected by the application?	___	___
d. Is input data validated and edited close to the point of origin to ensure the application rejects any incorrect transaction before its entry into the system?	___	___
e. Is all data that does not meet edit requirements rejected from future processing, reflected on an error message, and written to a suspense file?	___	___
f. Are error-handling procedures in place to facilitate the timely and accurate resubmission for processing of all corrected input data?	___	___

	YES	NO
g. Are change commands, rather than delete or erase commands, used to correct errors on the suspense file?	___	___
h. Are personnel with access to the system appropriately screened?	___	___
i. Are personnel granted access to only those resources and information required for their duties and no more?	___	___
j. Are personnel restricted from bypassing and overriding validation and editing problems?	___	___
k. Have personnel received security awareness training apprising them of the vulnerabilities of the application and techniques for enhancing security?	___	___
l. Is authorization of access (user identification, passwords, etc.) to the application actively managed by the user?	___	___
m. Is the identity of users verified prior to system access?	___	___

5. Data Processing Considerations. Data processing controls are used to ensure the accuracy, completeness, and timeliness of data during processing by the computer. "YES" responses to the following questions indicate low vulnerability to risk this area.

	YES	NO
a. Does the data center maintain a schedule showing when each application is to be run and needs to be completed?	___	___
b. Are computer-generated control totals (run-to-run totals) reconciled to check for com-pleteness of processing?	___	___
c. Do error-handling procedures identify erroneous transactions without processing them and without undue disruptions to the processing of other valid transactions?	___	___
d. Is operator intervention of data processing restricted?	___	___

	YES	NO
e. Is relationship editing performed between the input transaction and master files to check for appropriateness and correctness prior to updating?	___	___
f. Are there procedures for controlling the release of ADP storage media that have contained sensitive or classified information?	___	___

6. Data Output Considerations: Data output controls are used to ensure the integrity of output and the correct and timely distribution of outputs produced. Not only should outputs be accurate but they must be timely. Data can be output either by on-line or batch processing. "YES" responses to the following questions indicate low vulnerability to risk in this area.

	YES	NO
a. Are output reports reviewed for completenessand form?	___	___
b. Are outputs balanced to control totals withaudit trails available to facilitate tracing and reconciliation?	___	___
c. Are outputs controlled in accordance with written instructions?	___	___
d. Are outputs marked by appropriate security classification?	___	___
e. Are outputs marked in accordance with the level of sensitivity of the information?	___	___
f. Are procedures followed to report and control errors contained in output?	___	___
g. Does the user periodically verify the accuracy of all outputs?	___	___
h. Are appropriate methods used to dispose of documents that are not needed?	___	___
i. Are personnel with access to the output appropriately screened?	___	___

	YES	NO
j. Have personnel handling the output received security awareness training apprising them of the vulnerability of the application?	___	___

F. QUESTIONNAIRE 4 - ASSESSMENT OF INHERENT RISK. Questionnaire 4 was developed to help assess inherent risk. Analysis of each identified automated system must be performed to assess the potential for waste, loss, unauthorized use, or misappropriation due to the nature of the program itself. Matters to be included in the analysis are:

- Purpose and characteristics.
- Value of resources.
- Impact outside the agency.
- Age and life expectancy.
- Degree of centralization.
- Special concerns.

1. *Purpose and Characteristics Considerations*. The purpose and characteristics of the program being supported by the ADP operation or application should be considered to determine the degree to which it is susceptible to waste, loss, unauthorized use, mismanagement, or misappropriation. "YES" answers to the following questions indicate high vulnerability in this area.

	YES	NO
a. Is the program subject to:		
(1) Broad or vague legislative authority or regulations?	___	___
(2) Cumbersome legislative or regulatory requirements?	___	___
(3) Broad or vague missions, goals, or objective?	___	___
b. Is work assigned that often includes interaction with organizations outside managements' chain of command?	___	___
c. Do contractors perform work that could be considered Government work (e.g., a Government-owned project operated by a contractor)?	___	___

	YES	NO
d. Does the program involve handling classified or sensitive information?	___	___
e. Does the program involve handling valuable or sensitive inventory items or cash receipts or documents that can be used instead of cash?	___	___

2. Value of Resources Considerations. Programs or functions that require a large budget to operate and/or control or that disperse items of high value are more susceptible than lower budget programs to waste, loss, unauthorized use, or misappropriation. A "NO" answer to the following question indicates low vulnerability to risk in this area.

	YES	NO
a. Does the program require a large budget to operate and/or does it control or disburse items of high value? Items to be included:	___	___
(1) The annual operational cost (including salaries, hardware, software, etc.).	___	___
(2) The value of the items controlled (including data, property, funds, etc.).	___	___
(3) Value of the data supporting the program (costly to acquire or replace, highly valuable to outside sources, etc.).	___	___

3. Impact Outside the Program. If a program or function has a significant impact outside the activity, it may be subject to pressures to circumvent internal controls. A "NO" answer to the following question indicates low vulnerability in this area.

	YES	NO
a. Does the program or function have a significant impact outside the activity? Items to be considered include:	___	___
(1) The number of citizens impacted by the program.	___	___
(2) The impact on economic well-being of outside individuals or groups.	___	___

	YES	NO
(3) Impact on the health of outside individuals or groups.	___	___
(4) Impact on the safety of outside individuals or groups.	___	___

4. Age and Life Expectancy Considerations: The age and life expectancy of a program are factors to consider when analyzing risk. New or changing programs may lack written policies or procedures; lack adequate resources; have inexperienced managers and personnel; or lack devices to measure performance. Programs that are phasing out may lack adequate resources or involve close-out activities for which controls have not been developed, or involve accounting for significant amounts of money or other resources. "YES" answers to the following questions indicate low vulnerability in this area.

	YES	NO
a. Is the program in existence less than 2 years?	___	___
b. Is the program undergoing substantial modification or reorganization?	___	___
c. Will the program be eliminated within 2 years?	___	___

5. Degree of Centralization Considerations. The extent to which a program or function is operated in a centralized or decentralized manner should be determined. Excessive centralization of a program or function can increase the likelihood of loss due to fraud, waste, abuse, or mismanagement. "YES" responses to the following questions indicate low vulnerability to risk in this area:

	YES	NO
a. Is the program managed and controlled on a day-to-day basis? Factors to be considered include:	___	___
(1) Centralization (i.e., the program is managed and controlled on a day-to-day basis by Headquarters organizations or staff.)	___	___
(2) Decentralization (i.e., the program is managed and controlled on a day-to-day basis by field i nstallations or staff.)	___	___

	YES	NO
(3) Contractor administration (i.e., the program is managed and controlled on a day-to-day basis by a non-DoD organization.)	___	___
(4) Other (i.e., the program is managed and controlled by some combination of the above or by other means.)	___	___

6. Special Concerns. Often, the existence of special concerns for an activity may be indicative that for some reason it is highly susceptible to waste, loss, unauthorized use, or misappropriation, and should be treated as such. Consideration should be given as to whether the program or function has been the focus of special attention. "YES" responses to the following questions indicate low vulnerability to risk in this area.

	YES	NO
a. Has special interest in the program been exhibited by top executive officials, Congress, special interest groups or lobbyists?	___	___
b. Has the program received particular attention from the media?	___	___
c. Has the program been subject to recent litigation?	___	___

G. VULNERABILITY ASSESSMENT USING THE RESULTS.

1. The results of risk assessment questionnaires are used to:

a. Support management judgment as to the degree of risk involved,

b. Report weaknesses, and

c. Determine if more rigorous evaluation is needed.

2. Not all weaknesses are material in nature. In determining risk levels and in deciding on next steps, material weaknesses must be carefully considered in each agency's Management Control Plan. These Plans are required for each agency by 1987 in accordance with OMB Circular A-123 (reference (c)). Material weaknesses, if discovered, must also be included in prescribed annual reports to the President and Congress.

3. A material weakness is defined in reference (c) and the Internal Control Evaluation Guidelines as a situation in which the designed procedures or the degree of operational compliance, therewith, does not provide reasonable assurance that the objectives are being accomplished. The material weaknesses identified in the annual report should be of significance to warrant the attention of the President and Congress.

4. In the annual report to the President and Congress, the head of each agency must state whether the agency's systems comply with the Comptroller General's standards and must provide reasonable assurance that the objectives of internal control were achieved.

CHAPTER 6

ADP INTERNAL CONTROL TECHNIQUES

A. GENERAL

1. This chapter contains detailed ADP internal control techniques to be considered when developing or significantly modifying computer systems or applications. The section is divided among the three components of ADP internal control:

- Management Controls.
- Operations Controls.
- Application Controls.

2. The specific techniques are listed by element within these three areas. While the techniques in these areas generally apply to microcomputers, this Guideline separately presents internal control techniques specifically applicable to microcomputers; these techniques are presented in section D of this chapter. Users of microcomputers should refer to the techniques presented in section D. as well as those listed under Management Controls, Operations Controls, and Application Controls to ensure control over microcomputer operations.

3. It should be emphasized that the control techniques are listed only for consideration. It is left to the discretion of the reader to determine which techniques to apply based upon unique organizational and environmental characteristics and the related formulation of specific control objectives.

B. MANAGEMENT CONTROLS. Like any other resource, ADP needs to be properly managed to take full advantage of its capabilities. Managers should exercise sufficient control over the ADP function to determine how well it operates, where improvements are needed, and what capabilities will be needed in the future. To accomplish these objectives, control techniques that contribute to the effectiveness of the overall ADP program management should be considered as an element of the following areas:

- ADP Planning.
- Policies, Standards and Procedures.
- Organizational Controls.
- Internal Audit.

1. ADP Planning. The activities of the ADP organization should be part of planning the facility's overall operations.

ADP's objectives, both long- and short-range, should be consistent with those of the organization. The DoD process that applies in this area is Life-Cycle Management (LCM) and uses the principles set forth in DoD Directive 7920.1 and DoD Instruction 7920.2 (references (n) and (o)). The following techniques should be considered by ADP management to assure that ADP activities are properly planned.

a. An ADP management process that considers inputs from the various involved organizations, including major user departments and program areas, should be applied to:

(1) formulate policies for ADP systems;

(2) justify the need for new computer equipment; and

(3) assure that new equipment is acquired in the most economical and expeditious manner;

b. The facility should have formalized short- and long-range ADP plans;

c. The planning process should establish and document mission requirements, strategy, and overall system goals and objectives;

d. The ADP planning process should establish and document individual responsibility for specific actions to be undertaken;

e. ADP planning should be related to budgeting for financial, personnel, and system resources and to comparing and selecting among system alternatives based upon quantified life cycle cost, benefit, and risk projections;

f. The planning process should measure and compare actual accomplishments with expected performance throughout the system life-cycle;

g. Management should be informed of the status of planned actions through regular progress reports;

h. Regular internal audit review and reporting should be conducted regarding completed and proposed planning decisions in relation to mission requirements;

i. The ADP planning process should take into account relevant computer security requirements affecting the scope of ADP activity.

j. The ADP planning process should take into account approved agency records disposition schedules.

2. Policies, Standards and Procedures. Policies, standards, and procedures should exist and serve as the basis for management planning, control and evaluation. The following techniques should be considered to accomplish this objective:

a. The procedures for the ADP management process should be formally established;

b. All appropriate organizational components of the site involved with ADP systems should be defined and clearly assigned their respective areas of functional responsibility;

c. ADP resources acquisition, system design, programming, and operating standards should be established, coordinated and communicated to all affected personnel;

d. Policies to assist decision-makers in selecting among system development and operations alternatives (e.g., contracting versus in-house, shared versus separate facilities, purchase versus lease) should be established;

e. Procedures and responsibilities should be established for ensuring that, as applicable, OMB and GSA are apprised of ADP system initiatives;

f. Comprehensive ADP cost accounting procedures in accordance with GAO's Federal Government Accounting Pamphlet No. 4, "Guidelines for Accounting for Automatic Data Processing Costs," and OMB Circular A-130, Appendix II, "Cost Accounting, Cost Recovery and Inter-Agency Sharing of Data Processing Facilities" (reference (e)) should be established as appropriate;

g. Rigorous ADP budgeting procedures should be implemented to ensure that all significant ADP-related initiatives, expenditures, and reprogramming are clearly highlighted, whether or not they fall within budget decision units or are spread over multiple decision units;

h. Rigorous project control and performance measurement techniques (e.g., PERT, CPM) and progress reporting should be required based upon actual cost and work-year expenditures, deliverables provided, and milestones achieved (rather than upon subjective percent of completion estimates);

i. Policy and procedures should be established to comply with systems security, privacy, and freedom of information requirements;

j. Procedures describing the manner and responsibility for performance between users and ADP should be established, coordinated, and communicated to all affected organizations.

3. Organizational Controls. Effective controls need to be established over the data processing operation because of the concentration of functions brought about by the computer. The organizational structure should provide assurance that assets are safeguarded and that information is produced reliably. A key organizational control is an adequate separation of duties, which includes:

- Separating the data processing functions from other agency functions;

- Separating different data processing functions within the data processing organization;

- Providing for separation of duties within user departments.

Personnel capabilities need to be considered in determining which techniques are appropriate for establishing effective organizational controls. The following techniques should be considered to implement effective organizational controls over the ADP function:

a. The ADP function should be placed sufficiently high in the organization to ensure its independence from other site operations;

b. All ADP employees should be prohibited from having authority or duties in any other organization without management approval;

c. Major organizational units within ADP should be described and their responsibilities delineated and documented;

d. Where practical, the following functions should be performed by a different individual or group:

- Systems analysis.

- Application programming.

- Acceptance testing.

- Program change control.

- Data control.

- Production control and scheduling.

- Computer equipment operation.

- System software maintenance.

- Computer files maintenance.

- Source document origination.

- Source document conversion to machine-readable format.

e. Transactions generally should originate and be authorized in an organization outside of ADP;

f. A direct line of responsibility should exist between every subordinate and supervisor;

g. A personnel rotation plan should be in effect within the different functional areas in the ADP organization;

h. ADP personnel should be required to take regularly scheduled vacations;

i. Absentee and turnover rates in the ADP organization should be monitored for potential personnel problems;

j. ADP position descriptions should be in writing, be clear in delineating authority and responsibility, be kept current, be accompanied by definitions of technical skills needed, and be usable as a basis for performance evaluation;

k. Personnel recruiting and promotion practices should be based on objective criteria and should consider education, experience, and security risks relevant to the job requirements and to the degree of responsibility;

l. Before being hired, ADP personnel should be subjected to preemployment checks;

m. When hired, employees should be provided with an orientation of internal controls and security and with ongoing training to maintain their technical knowledge, skills, and abilities;

n. Training programs should exist to maintain and build skills, knowledge, and ability in systems technology, internal control, and ADP security requirements;

o. Employee performance should be evaluated on a regular basis, and any negative performance should be appropriately addressed.

4. Internal Audit. The Component's internal audit staff should be responsible for assuring top management that systems are developed in accordance with objectives, contain the needed internal controls to produce consistently reliable results, and operate in conformance with management standards and approved design specifications.

a. The internal auditors charter should allow the conduct of independent reviews and the reporting of findings and recommendations to the site's management;

b. The responsibility of the internal audit function in relation to ADP should be clearly documented;

c. Internal Audit should actively participate in reviewing the development of new systems or applications and the significant modification of existing systems;

d. During system planning and development, internal audit should ensure that the system carries out prescribed management policies;

e. Internal audit should review general controls in data processing systems to determine that controls have been designed according to management direction and legal requirements and that these controls are operating effectively to provide reliability of, and security over, the data being processed;

f. Internal audit should review application controls of computer-based systems to assess their reliability in processing data in a timely, accurate, and complete manner;

g. These control reviews should ascertain whether the systems conform to both organization and Federal standards;

h. Periodic audits should be designed to test both internal controls and reliability of processed data;

i. When appropriate, Internal audit should verify the information on output reports against related source documents.

C. OPERATIONS CONTROLS. Operations controls apply to all processing carried out within a computer installation and are independent of any specific application. Operations controls include:

- Data center operations controls;
- Security controls;
- System software controls;
- Hardware controls; and
- Distributed processing and network operation controls.

The effectiveness of these controls are of high importance in the ADP environment because weaknesses can affect all processed applications.

1. Data Center Operation Controls. Control procedures concerning data center operations should be established and followed to ensure accuracy and completeness of the information maintained and processed by the ADP facilities. These controls should be to prevent errors in data preparation and handling and aid in production scheduling, file updating, and output report preparation. Strong controls in specific key areas will help prevent or decrease the probability of inaccurate or fraudulent processing. Data center operations controls can be broken down into the following areas:

- Work Load Scheduling Controls.

- Malfunction Reporting and Preventive Maintenance Controls.

- User Billing/Charge-back Controls.

a. Work Load Scheduling Controls. Control procedures over work load scheduling and the inputting and outputting of data should be enacted and complied with. Certain production scheduling and input and/or output controls may be bypassed when remote job entry devices are used to schedule. However, a control group should monitor and manage these operations. The following control techniques should be considered to ensure that proper controls are being maintained over workload scheduling:

(1) A formal control group should be established within the data center to monitor both remote decentralized as well as centralized job entry;

(2) Formal input and/or output control procedures should be established and documented;

(3) All personnel should have a copy of a manual detailing required control procedures;

(4) The control group should be responsible for recording and controlling the production data processed by the data processing organization;

(5) All totals should be balanced during and after applications processing, and all processing errors should be controlled by the control group;

(6) An authorization document or a transmittal sheet should be required to accompany all input transactions;

(7) All output reports should be visually scanned by the control group for general accuracy and completeness and be distributed according to a formal schedule;

(8) The control group should establish and document formal scheduling procedures, schedule production runs

and other workloads, and reschedule aborted or erroneous processing;

(9) A priority scheme of classes or priorities should be used for scheduling work;

(10) A schedule of all computer-based systems should exist and include a brief description of the function of each system, the date of approval, and an identification number;

(11) Source documents should be maintained for reference in a logical sequence for a suitable period of time;

(12) All characteristics of jobs (run time, data sets, access time, computer devices required, etc.) within the job stream should be defined and documented;

(13) The mix of on-line and batch jobs should be scheduled in order to promote efficient use of facilities and to meet user requirements;

(14) A systematic time-related flow of jobs through each work center should be established;

(15) Users should be involved with workload scheduling, except in emergencies;

(16) Operators should not be involved with workload scheduling, except in emergencies;

(17) Rush or rerun jobs should be scheduled consistent with their priority ratings;

(18) Reasons for schedule delays should be identified by area of responsibility;

(19) Approximate elapsed time of delay should be recorded for each delay event;

(20) In on-line systems, response time statistics should be kept and monitored for significant fluctuations in response time;

(21) CPU utilization statistics should be monitored for both batch and on-line processing;

(22) Significant variances in performance should be followed up by the control group.

b. Malfunction Reporting and Preventive Maintenance Controls.

(1) Control procedures concerning malfunction reporting and preventive maintenance should be established and

followed. Malfunction reporting should ensure that errors and omissions resulting from hardware or software system crashes are reported. In addition, it should provide measures of the adequacy of the preventive maintenance, of the level of vendor maintenance provided, and of the failure rate of the system. Preventive maintenance should be performed according to established facility and vendor procedures.

(2) The following control techniques should be considered to ensure that proper controls are being maintained over malfunc-tions reporting and preventive maintenance:

(a) Formal malfunction reporting procedures should be established and documented for the data processing installation;

(b) Operators and all other appropriate personnel should have access to a manual detailing these control procedures and certify in writing that they have reviewed and understood them;

(c) These logs should record start ups, errors, reruns, recoveries, shut downs, shift changes, and maintenance occurrences;

(d) Log pages should be sequentially numbered;

(e) The computer system should automatically produce a log of all system operations;

(f) The console log should include the date, job name and number, program name and number, start and/or stop times, files used, record counts, and scheduled and unscheduled halts;

(g) Disposition notes should be entered on the console log showing corrective actions taken when unscheduled program halts occur;

(h) Job reruns should be recorded along with their reason on the console log;

(i) Console log pages should be sequentially numbered;

(j) Logs should be reviewed and signed at the end of each shift by a supervisor and filed as a permanent record;

(k) Logs should be independently examined to detect operator problem and unauthorized intervention;

(l) System crashes should be isolated and identified by cause;

(m) System reliability reports should include Mean Time Between Failures (MTBF) and Mean Time to Recovery (MTTR) statistics;

(n) System performance records should be maintained;

(o) Formal preventive maintenance procedures should be established and documented for the data processing organization;

(p) Logs of the type and time of maintenance performed should be kept;

(q) A schedule for machine maintenance should be published and followed;

(r) Sensitive data should be removed from on-line storage devices before equipment is turned over to maintenance personnel;

(s) The production schedule should be flexible enough to accommodate preventive maintenance;

(t) Preventive maintenance should not be scheduled during peak load periods.

c. User Billing and Charge-back Controls.

(1) Control procedures over user billing and charge-back should be established and complied with. Controls should be designed to encourage appropriate usage of computer resources and fair treatment of users and their needs. All costs should be derived on a fair and equitable basis in accordance with management policy and procedures and with Federal guidelines.

(2) The following control techniques should be considered to ensure that proper controls are being maintained over user billing and charge-back procedures:

(a) Procedures for user billing and charge should be documented;

(b) Billing and charge-back agreements should exist between users and the data processing organization;

(c) The user billing charge-back procedures should be effectively tied into a job accounting system for the data processing resources;

(d) The user billing and charge-back procedures should be based on the number of transactions

processed, on an artificial "computer accounting unit," or some other equitable method;

(e) Adequate procedures should exist for determining the share of system development costs plus additional overhead items, such as lighting, space, and air conditioning, for billing users;

(f) Additions and replacements of hardware, software, etc. should be justified on the basis of resource utilization and user needs;

(g) An equitable procedure should exist for charging reruns of productions jobs so that user errors are charged back to users, while data processing organization errors are absorbed by data processing;

(h) Current data processing organization costs should be consistent with budgeted costs;

(i) Periodic billing statements should be provided to user departments describing cost details and the billing algorithm used;

(j) Rates charged to users should encourage the use of data center resources in accordance with users' needs; differential rates for off-peak usage or the assignment of processing priorities for varying turnaround requirements should be used to encourage maximum usage of centralized computer facilities.

2. Security Controls. Control procedures concerning computer security should be enacted and followed to protect and safeguard ADP resources. The hardware, software, and data are all assets that should be managed properly and protected against theft, loss, unauthorized manipulation, fraudulent activities, and natural disasters. To minimize these risks, controls to limit access to the data center, decentralized hardware, system and application programs, system documentation, and outputs should be established. Site management should also establish and enforce strict procedures over maintenance, storage, and access to data storage media as well as preventive procedures that help protect critical files, programs, and system documentation from natural disasters. Security controls can be broken down into the following areas;

- Administrative Controls;
- Physical Controls;
- Technical Controls;
- Disaster Recovery Controls.

Control techniques that should be considered in each of these areas are presented in the following sections.

a. Administrative Controls. The following techniques should be considered to effectively administer the ADP security function.

(1) Responsibility for conducting risk analyses should be formally assigned.

(2) Responsibility should be assigned for computer security at each ADP facility;

(3) Individuals assigned responsibility for computer security should be given training and experience in both the computer and security areas;

(4) Risk analysis studies should measure vulnerability related to the potential for the following:

(a) Fraud or theft,

(b) Inadvertent error or improper disclosure of information,

(c) Financial loss,

(e) Harm to individuals or infringement on privacy rights,

(f) Loss of proprietary data and harm to organizational activities;

(5) A specific timetable for conducting risk analysis studies should be established, with the time between studies being commensurate with the sensitivity of the information processed;

(6) Risk analysis studies should be performed at least every 5 years;

(7) Procedures should require that a risk analysis be performed before the approval of design specifications for computer installations or whenever significant changes are made to the physical facility, hardware, or operating system software;

(8) Requirements should be established for conducting risk analysis for DoD government-owned, contractor-operated facilities and for Government-operated facilities;

(9) Plans should provide for assessing risks related to computer services provided by other agencies and those provided through commercial services;

(10) Employees utilizing ADP equipment and processing DoD data should be required to sign an agreement regarding their role and responsibility at the facility and in the ownership and use of data processing equipment and information within the data center;

(11) ersonnel security policies for screening employees and contractor and/or service personnel should be established and provide for levels of screening commensurate with the sensitivity of the position or function;

(12) When an employee is terminated, the employee should immediately be denied access to the data processing organization, any data, program listings, etc.; and all other employees should be informed of the employee's termination;

(13) Procedures should exist to handle a situation in which an employee becomes a suspected security risk.

b. Physical Controls. In order to reduce the risk of erroneous or fraudulent activities, physical security controls should exist to protect ADP resources against unauthorized access. The following physical security control techniques should be considered to accomplish this objective:

(1) Written procedures should exist to define restrictions to computer room access;

(2) A reliable guard service or alarm system should exist to protect the computer center against illegal entry, vandalism, or sabotage;

(3) Access to the computer areas should be restricted to only authorized and appropriated personnel through the use of a passcard system, combination locks, security badges, or other appropriate secure means;

(4) Combinations on locks or similar devices should periodically be changed;

(5) Account codes, authorization codes, passwords, etc. should be controlled to prevent unauthorized use;

(6) Restricted entrances and emergency exits should be equipped with tamperproof automatic alarm systems that signal when doors are opened;

(7) Exterior walls, tape library walls, storage room walls, etc, should be of solid construction from floor to ceiling;

(8) Data processing personnel should be trained to challenge improperly identified visitors;

(9) Data processing personnel should be counseled to report all intentional or inadvertent cases of security intrusions of which they become aware;

(10) Access to the computer area by custodial, electrical and other in-house maintenance personnel should be supervised and controlled;

(11) Vendor and support personnel should provide positive identification before they can be admitted to the computer area;

(12) At least two individuals should be present in the computer room at all times;

(13) A procedure should exist to restrict access to source documents and blank input forms to authorized employees;

(14) All critical forms, such as identification cards, negotiable instruments, and source documents, should be prenumbered for accountability, stored in a secure location and periodically accounted for;

(15) Procedures should exist to limit access to critical forms during their intermediate storage and transportation, such as dual custody and mail message carrier controls;

(16) A procedure should exist for joint authorization of releases from the storage areas, and the receipt of critical forms should be inventoried by two people at the time of delivery;

(17) Procedures should be established to control the issuance of critical forms for jobs scheduled for processing;

(18) Copies of critical outputs that need to be destroyed should be kept in a secure location until they can be destroyed;

(19) At least two people should be present when critical outputs are destroyed.

c. Technical Controls. Control procedures over system and file access should be established and followed. The use of system security software, as well as of a librarian function, will reduce the possibility of illegal system access and erroneous or fraudulent processing. The following techniques should be considered to ensure systems security:

(1) Separate security software should be used to provide control over the site's computer resource;

(2) The vendor or developer of the security software should provide a completely documented description of its design and operation;

(3) The security software should control access to terminals, remote job entry station, individual automated data files, application programs, and other system software;

(4) Security software functions should be adequately supported by proper manual procedures;

(5) The control functions performed by security software should not be able to be overridden or bypassed;

(6) The security software should provide an audit trail of all authorized uses and unauthorized attempted accesses of computer resources under control;

(7) the security software should control access to data in a different manner than access to other computer resources;

(8) The security software should be transparent to all application programs and to all other system software;

(9) A list of all personnel should exist and be periodically reviewed by supervisors detailing what computer resources the personnel have access to;

(10) On an on-line environment, there should be access security control based on the classification of file data and devices;

(11) The responsibility for issuing and storing disk packs, magnetic tapes, or other data storage media should be assigned to a librarian;

(12) The responsibility referenced in item 11, above, should be the librarian's chief function;

(13) Library procedures should be documented;

(14) Access to the library should be limited to authorized personnel;

(15) A librarian should be on duty whenever the data center is being used;

(16) Sensitive files, such as security classifications or Privacy Act restrictions (reference (1)),

should be properly identified as such, and appropriately secured;

(17) To prevent release to unauthorized personnel, all data files should be logged in and out;

(18) All files should be expeditiously returned to the library after use;

(19) Disk packs and tape inventory records should be kept;

(20) External labeling procedures should be documented;

(21) External labels should be affixed to active disks and/or tapes;

(22) Work or scratch tapes should be kept in separate area of the library.

d. Disaster Avoidance and Recovery. Control procedures concerning disaster recovery should be established and followed. Controls should help prevent fire or other natural disasters from destroying hardware, critical files, programs and system documentation. If a disaster were to occur, a disaster recovery plan should be implemented to ensure the recapture of critical information. These control procedures need to be formally documented and periodically tested and updated. The following techniques should be considered to minimize the impact of unanticipated interruptions:

(1) Emergency procedures should be formally documented and distributed to all associated personnel;

(2) Procedures should include steps to be taken in the event of an actual or likely natural disaster by fire, water damage, etc., and intentional damage by sabotage, mob action, bomb threats, etc.;

(3) The computer center should be separated from adjacent areas by fire resistant partitions and/or walls, and noncombustable flooring, ceilings, furniture, carpets and draperies should be used;

(4) Smoking should be prohibited in the data center;

(5) Data center personnel should be trained periodically in firefighting techniques and be assigned individual responsibilities in case of fire;

(6) Emergency procedures for handling minor and major fires should be prominently posted throughout the data center;

(7) Heat and smoke detectors should be installed in the ceiling, under raised floors and in the air ducts, alerting the local fire department as well as internal personnel;

(8) Portable fire extinguishers should be located in strategic and accessible areas, be vividly marked, and periodically tested;

(9) Emergency exits and evacuation routes should be clearly labeled, and battery-powered emergency lights placed in strategic locations to assist in evacuation if the power should be interrupted;

(10) The computer center should be protected by an automatic fire suppression system;

(11) Emergency switches for cutting off power should be easily accessible near the data center exits;

(12) Emergency power shutdown should include the air conditioning system;

(13) Either the computer center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and humidity in the computer center and take appropriate actions as necessary;

(14) The computer center should be air conditioned by a separate system sufficiently protected from unauthorized access and made from noncombustible materials;

(15) Air intakes should be protected against the introduction of noxious substances;

(16) Backup air conditioning should be available;

(17) The source of electric power should be sufficiently reliable to assure continued operations and be adequately protected from unauthorized access;

(18) The computer center should be backed up by an uninterruptible power source system;

(19) Procedures should exist and be applied for the retaining and/or copying of master files as a means of reconstructing a damaged or destroyed file;

(20) Sufficient generations of files should be maintained to facilitate reconstruction of records;

(21) At least one file generation should be kept at a location other than the file storage area;

(22) Copies of critical files, application programs, system software programs and critical documentation should be stored at an off-site location and be restricted from unauthorized access;

(23) Backup computer capacity should exist within the computer center and at an off-site location;

(24) Critical locations should be provided with the backup devices of terminals, modems, and communication lines;

(25) Backup arrangements should be documented and formally agreed upon by all parties concerned;

(26) A priority scheme should be established at the site and be approved by management, in the event that backup arrangements must be used;

(27) Backup procedures should be periodically tested;

(28) Off-site materials should be kept up-to-date;

3. System Software Controls. Control procedures concerning system software should be established and followed. Controls should ensure that the system software provides security and integrity of the system. A systematic procedure should be enacted to identify all potential system software programs that will satisfy organizational requirements. A thorough cost and/or benefit analysis of system alternatives should be used to identify the most effective system. The software should be comprehensively tested prior to release for production. System software controls can be separated into the following categories.

- Operating Systems.
- System Utilities.
- Program Library Systems.
- File Maintenance Systems.
- Data Communication Systems.
- Data Base Management Systems.

- System Software Change Controls.

Control techniques for each of these areas are detailed in the following sections:

a. Operating Systems Controls. Control procedures concerning operating systems should ensure that a quality operating package is in place and is managed and operated correctly. The following techniques should be considered to ensure proper controls over the operating system:

(1) A complete documented description of the operating system's design and operation should be provided by the vendor or developer;

(2) The operating system should prohibit one application program from accessing memory or data of another application program that is processing simultaneously;

(3) The operating system should prohibit an application program from accessing operating system instructions, password tables and other security algorithms;

(4) The operating system should prohibit operators from entering application data or changing users' memory values at the computer console;

(5) The use of privileged instruction of the operating system should be strictly controlled;

(6) The operating system should control all input and/or output functions of data files;

(7) Operating system instructions, password tables, and other authorization algorithms should be protected form unauthorized access when the computer system fails;

(8) The integrity of the operating system should be tested after initial installation;

(9) The operating system should prohibit application programs from overriding or bypassing errors that are detected during processing;

(10) All application programs or other system software should be run only when the operating system is operational;

(11) An audit trail of all operating system actions should be maintained either on the automatic console log or as part of the computer system's job accounting data;

(12) The computer system's internal clock should be adequately protected from unauthorized access;

(13) The operating system should adequately and accurately schedule all jobs run on the computer system.

b. System Utilities Controls. Control procedures over system utilities should be established and controlled. The following techniques should be considered to ensure proper controls over the sue and operation of system utilities:

(1) The vendor or developer of the system utilities should provide a complete documented description of their design and operation;

(2) A complete directory of all available utilities should exist;

(3) Computer operators should be denied access to system utility documentation;

(4) Management authorization should be required prior to the installation and use of new releases of utility programs;

(5) Controls that detect processing errors in system utilities should not be able to be overridden or bypassed;

(6) System utilities should not be able to be used to override or bypass controls within other system software or application programs.

c. Program Library Systems Controls. Control procedures over program libraries should be established and followed. The following techniques should be considered to ensure controls over automated program libraries:

(1) A program library system should be used to control application programs;

(2) The vendor or developer of the program library system should provide a complete documented description of the system's design and operation;

(3) The program library system should restrict access to application programs, control movement of programs from test to production modes, control movement of programs form source code to object code, and control changes to application programs;

(4) Program library system functions should be adequately supported by proper manual procedures;

(5) Control functions performed by the program library system should be protected so they cannot be bypassed;

(6) The program library system should provide an audit trail of all changes made to application programs;

(7) The program library system should prevent the existence of more than one version of a source code and object code program;

(8) Obsolete programs should regularly be deleted from the source code and object code library;

(9) Computer operators should be denied access to all libraries maintained by the program library system.

d. File Maintenance Systems Controls. Control procedures covering file maintenance systems should be enacted and followed. Controls ensure that a quality file maintenance system is in place and properly used. The following techniques should be considered to ensure proper control over file maintenance systems:

(1) A file maintenance system should be used to control all disk and tape data set;

(2) The vendor or developer of the file maintenance system should provide a complete documented description of its design and operation;

(3) The file maintenance system should control the establishment, use, and retention of automated data files;

(4) File maintenance system functions should be adequately supported by proper manual procedures;

(5) Control functions performed by the file maintenance system should be protected so that they cannot be overridden or bypassed;

(6) The file maintenance system should include redundancy controls, such as prohibiting more than one data file from having the same volume serial number;

(7) The file maintenance system should provide an audit trail of all uses and accesses of all automated data files.

e. Data Communications Systems Controls. Control procedures over data communications systems should be enacted and implemented. Controls should provide assurance against both illegal access and erroneous data transmission. The following techniques should be considered to control the operation and use of data communications systems:

(1) A data communications system should serve as the interface between terminals and the central data processing system;

(2) The vendor or developer of the data communications system should provide a complete documented description of its design and operation;

(3) The data communications system should control access to and use of terminals, poll and receive messages from computer terminals or other computers, address and send messages back to computer terminals or other computers, edit and format input and output messages, handle error situations, reroute traffic when terminals or lines are inoperative, and perform on-line formatting on visual display terminals;

(4) Data communications system functions should be adequately supported by proper documented procedures;

(5) Functions of the data communications system should be protected so that they cannot be overridden or bypassed;

(6) A built-in hardware identification code should be checked by the data communications system to ensure that no unauthorized terminals are being used;

(7) The data communications system should use a table of authorized terminal addresses to allow polling with the communications network;

(8) User authorization codes or passwords should be required by the data communications system to access the computer system and application programs, other system software and to enter transactions;

(9) Different authorization codes should be required to enter different types of transactions;

(10) The authorization code should identify the individual using the terminal and should be periodically changed;

(11) A nonprinting and/or nondisplaying facility should be used when keying in and acknowledging user authorization codes;

(12) A terminal identification check should be performed by the data communications system so that various transaction types can be limited to authorized data entry stations;

(13) The security matrix or table used to control access to the application system should be properly protected to prevent unauthorized access;

(14) A message header should be used by the data communications system to identify the source of the message, including proper terminal and use authorization code, message sequence number, including total number of message segments,transportation type code and transportation authorization code;

(15) This message header should be validated by the data communications system;

(16) The data communications system should include an end-of-transmission trailor that includes message and segment, value totals, including debits and credits, and an ending symbol;

(17) The data communications systems should reconcile counts and totals with header counts and totals;

(18) The data communications system should send acknowledgments to the terminal indicating receipt of messages and periodically test line and terminal operating status with standardized test messages and responses;

(19) The data communications system should use buffering to queue messages when a device, such as a terminal, is busy;

(20) The data communications system should maintain a transaction log of sequentially numbered and/or time-of-day-noted transactions;

(21) The transaction log should record the originating terminal, user authorization code, message identification, transaction type code, time of day that the transaction was logged, and transaction data;

(22) The transaction log should provide part of the audit trail, account for all error messages, and record, with control totals, all retrievals made by a particular terminal;

(23) All messages awaiting transmissions should be logged by the data communications system before being put into the transmission queue and then purged after transmission.

f. Data Base Management Systems Controls. Control procedures concerning data base management systems should be established and followed. Controls should provide assurance of the quality as well as the use of the DBMS. The following

techniques should be considered to control the operation and use of data base management systems:

(1) Where appropriate, responsibility for administering the data base environment should be established at a high enough level to ensure independence;

(2) The vendor or developer of the data base management system should provide a complete documented description of its design and operation;

(3) The data base management system should provide security over data base accesses; control the addition, modification, and deletion of data; and provide a complete documented description of its design and operation;

(4) Integrity of data maintained within the data base should be ensured thorough utility programs that check the physical linkage of data within the database, control records that maintain interim balances of transactions, and apply application programming standards that include procedures for maintaining integrity;

(5) Data base management system functions should be adequately supported by proper documented procedures;

(6) Functions of the data base management system should be protected so that they cannot be overridden or bypassed;

(7) The use of restricted instructions should be logged and checked periodically;

(8) The data base management system should use authorization codes or passwords to control access to data items;

(9) The data base management system should record unsuccessful attempts to access the data base;

(10) The data base management system should record which application programs have accessed each data item within the data base;

(11) The data base management system should prevent simultaneous updates to a record;

(12) The data base management system should prevent shared data from being deleted without consent of all users of the data;

(13) A log should indicate whether an application program has read, updated, created, or deleted a data item;

(14) All errors discovered by the data base management system should be logged for follow-up;

(15) Failures in the data base management system should be documented for supervisory review;

(16) A data dictionary should be developed and maintained, documenting the attributes of each data item and the security over each data item.

g. System Software Change Controls. Control procedures concerning system software changes should be established and followed. Controls should prevent unauthorized or inaccurate software changed. The following techniques should be considered to control system software changes:

(1) Formal documented system software change procedures should be established;

(2) Change request forms or other documentation should be used to originated system software modifications, with all forms sequentially numbered and accounted for;

(3) System software changes should be thoroughly tested to ensure that modifications function properly;

(4) System software modifications should be subjected to a system acceptance test before being placed in operations;

(5) All relevant documentation should be changed to reflect system software modifications;

(6) The volume of regularly scheduled system software modifications should be monitored and examined as an indicator of potential problems with the software, procedures or application;

(7) Computer operation personnel should have a list of system programmers to notify if the system software requires an emergency or immediate modification;

(8) Access to data files and application programs should be denied to the system programmer making a system software modification;

(9) The system programmer making an emergency modification should be denied access to data files and application programs that were operating when the problem occurred;

(10) The system programmer making an emergency system software modification should complete a signed statement

and leave it with the computer operator as to the encountered problem and its solution;

(11) Procedures should be established to ensure that emergency system software modifications are immediately subjected to a system acceptance test;

(12) Procedures should be established so that the accepted emergency modifications will be incorporated into the next operational version of the system software.

4. Hardware Controls. Hardware controls should be included by the manufacturer in the design of the computer equipment. Although computers possess a high degree of reliability, the potential for malfunction does exist. Hardware should be frequently checked to ensure that protection features are operating properly and have not been disabled. When equipment malfunctions, it should be recorded and reported to the vendor. An inventory of various features of all equipment should be kept, including location, model number, identification number, type and speed.Hardware controls should ensure the accuracy and reliability of computer processing. Although users and managers of ADP operations do not have much choice in this area, it is included for design or procuremnt considerations. Hardware control consist of:

- CPU Control.
- Peripheral Controls.
- Data Communication Controls.

a. Central Processing Unit Controls. Controls should be built into the design of the control processing unit. Controls should ensure the accurate transmission of data and that only valid operation occurs. The following control techniques should exist within the CPU:

(1) Built-in parity bits should be used by the CPU to ensure that all data elements transmitted through the internal circuitry are correctly transmitted;

(2) Redundant character checking should be used by the CPU to insure the correctness of data processing;

(3) The CPU should use validity checks to ensure that only valid operation codes are used;

(4) The CPU should perform validity checks on the numbers used to access memory to insure that only valid numbers are used;

(5) The CPU should have automatic interlock controls to prevent the equipment from performing certain operations at the wrong time;

(6) Log should be maintained to record CPU meter readings at the start and end of each shift, and variances should be explained.

b. Peripherals Controls. Hardware controls should be built into peripherals to ensure the accurate transmission of data and the valid occurrence of operations. The following control techniques should exist within the peripherals:

(1) Parity checks of both individual and blocks of data should be made to ensure that all data elements are transmitted accurately;

(2) Validity check controls should be used to check the results of an operation with all possible valid solutions;

(3) Echo checks should be used to ensure that a transmitted command is actually performed or the data sent is correct;

(4) A read-after-write check should be used to ensure that the record just written was correctly recorded;

(5) Equipment diagnostic tests should exist for the computer to check if the equipment is functioning properly;

(6) With direct access storage devices, address comparisons should be made to verify the address to which data is to be written with the address called for by the instruction;

(7) Print synchronization controls should be used to check the timing of the printer to determine that print hammers of impact printers are activated at the moment when appropriate characters are in the correct position.

c. Data Communications Controls. Controls over data communication devices should be established and followed to ensure accuracy and privacy of transmitted data. The following control techniques should exist within data communication devices:

(1) A unique hard-wired identification code, requiring no human intervention for its use, should be incorporated into each terminal device;

(2) The identification code should be checked and validated by the computer to ensure that no unauthorized terminals are being used;

(3) Data communications lines should be conditioned for improved accuracy and physical security;

(4) Scrambling or encryption techniques should be used in transmitting classified data;

(5) An automatic store-and-forward capability should be used to maintain control over messages queued for an inoperative or for a busy communications device;

(6) A message intercept function should be used to receive messages directed to inoperable or unauthorized terminals;

(7) Parity checks should be used to detect errors in the transmission of data;

(8) Validity checks should be used to compare character so that erroneous data can be detected;

(9) Echo checking should be used to verify each character so that erroneous data can be detected;

(10) Forward error correcting techniques should be used for the detection and reporting of data communications errors using sophisticated redundancy codes;

(11) Techniques should be available for detecting erroneous retransmissions of data;

(12) Modems should be equipped with loop-back switches for fault isolation.

5. Distributed Processing and Network Operations Controls.

a. Control procedures concerning distributed processing and network operations should be formally established and followed. With the rapid increase of decentralization of systems and network operations, high risk areas of data security and integrity have become major concerns.

b. The following control techniques should be considered to ensure proper controls over distributed processing and network operations:

(1) The decision to undertake distributed processing should be documented and supported by cost and/or benefit analysis studies;

(2) The distributed processing requirements definitions should be responsive to management objectives in terms of the hardware configuration, data base configuration and hardware and communications network interface;

(3) A network implementation, conversion, and acceptance plan should be developed jointly by systems and network user organizations and include user-prescribed test procedures and acceptance criteria;

(4) Users should participate in acceptance test, review test results, and provide approvals for functions over which they have jurisdiction;

(5) The operating provisions in the implementation plan should be consistent with the laws and regulations governing transmission of data within the country and/or internationally;

(6) Standards and policies for general network control should be clearly established and followed;

(7) Network standards and policies should be sufficiently broad-based, not to encumber local autonomy or operating objectives;

(8) As the general network capability is distributed, controls should be distributed to users;

(9) A network policy should require the ongoing identification of data set needing inter-system compatibility;

(10) A network should exist requiring audit trails and backup of all network communications activity for both network messages and application processed data;

(11) A network data review mechanism should be established to administer compatibility between system and data as the network grows;

(12) Hardware controls should include memory protection, alternate communication routing, communication protocols and timely failure recovery mechanisms;

(13) Software controls over reentrant operating systems and current data base accesses and update should exist;

(14) External labels should be used on cables, modems, control units, and other hardware devices to expedite fault isolation and service;

(15) Adequate controls and training regarding distributed data should exist to ensure data compatibility, integrity and effective data usage;

(16) Appropriate techniques and policies should be instituted for standardizing data definitions of shared data, maintaining common data dictionaries, and reconciling deviations in data definition at remote facilities;

(17) Network data policies should require that data set ownership be clearly established;

(18) User and system responsibilities should be fully defined for coordinating and reconciling differences between distributed and/or replicated data bases prior to network implementation;

(19) Reconciliations should be able to be satisfactory performed under normal conditions, following network failures, and between varying application problems;

(20) Commonly shared and distributed data should be designed to readily permit integration and summarization at an organization-wide level to meet current or anticipated objectives;

(21) Network data standards should require and define data set change control procedures;

(22) Documentation and training should be provided to all network operations personnel;

(23) Adequate security should exist and be periodically reviewed over data controlled by network data base management systems and application and/or transaction processor, and over data handled at network processing facilities and remote locations;

(24) Review procedures for identifying and handling sensitive data should exist, and security classification for all levels of data sets in the network should be developed, consistent with information classification requirements;

(25) Procedures stating the preferred method for disposing of sensitive network documents at remote locations should exist and be communicated to the appropriate personnel;

(26) A central control function should be established to coordinate control reviews of network assets and resources at all network locations;

(27) Network asset inventories should be maintained at respective facilities and be periodically reviewed against actual network facilities;

(28) Control reviews should be used for assessing the ongoing integrity and overall control of the physical network;

(29) Summary control reports should be distributed to all network user organizations;

(30) Effective hardware and software backup provisions should exist for the entire network and for the individual facility;

(31) Adequate disaster and recovery procedures should be developed for each network processing facility; these procedures should be current and periodically tested;

(32) Written procedures should exist for switching to backup equipment, files, or systems;

(33) Network output requirements, operating schedules, processing procedures, and facility coordination policies should be fully established;

(34) Network availability and reporting, timing and/or response, storage, backup, and functional control requirements for all applications should be established by users and communicated to the responsible network operations organization;

(35) All network facilities should communicate with each other on a regular basis to discuss schedules and coordinate processing requirements and operating procedures;

(36) All network facilities should prepare schedules of consumable needs so that resources can be efficiently and effectively distributed throughout the network;

(37) Records should be maintained on the amount of resources used by each facility;

(38) All network locations should receive regularly scheduled hardware preventive maintenance and log all hardware problems;

(39) Remote and local network control terminals, and operations personnel authorized to use them, should be identified;

(40) Policy agreements should exist for communications transmissions including provisions to effectively interface software applications and data bases among coordinated network facilities;

(41) Each network message and/or transmitted data unit should contain codes that identify the sender and intended receiver(s);

(42) All outgoing messages and/or data units should be edited for valid destination addresses;

(43) Communications provisions should exist to temporarily store messages and/or data units destined for remote facilities not in service and for reactivating them when service is resumed;

(44) The assignment of transmission priorities should be consistent with established policy and appropriate for the need of the on-line application;

(45) All changes made to network operating systems software at remote processing facilities should be controlled by the central and/or main network processing facilities;

(46) Procedures should exist at remote facilities to ensure that all changes made to operating systems software are effectively controlled and made immediately visible to the control group directly responsible for the overall network;

(47) Proper access control should be maintained over the storage and use of network test equipment;

(48) Local and/or private communications lines and switches should be adequately secured and accessible only by authorized personnel;

(49) A cost and/or benefit analysis of encryption and private line acquisition should be made;

(50) When encryption is in use, the individual assigned the responsibility of management should not be involved with the operation or processing of data;

(51) Consolidated security reports should be periodically published reflecting recent network security reviews, and they should be available to all network user organizations;

(52) Remote users should have a list of standard terminal, modem, and controller device settings to facilitate problem determination;

(53) A comprehensive post-implementation technical review of the network should be required and performed by systems personnel;

(54) Local and consolidated network performance reports should be established to regularly report key elements such as network system availability, performance to schedules, response times, processing facility efficiencies and performance problems;

(55) Adequate security measures should be in force at the backup facility.

D. APPLICATION CONTROLS

1. General.

a. Application controls are primarily concerned with data being processed. Collectively, they form a network of controls in a system to facilitate the production of accurate and reliable information. Certain internal control techniques should be incorporated directly into the applications to help ensure accurate and reliable processing. Although these control techniques may be unique to a particular applications, they can normally be grouped according to various stages of data processing. The basic application control techniques consist of:

- System Design, Development and Modification Controls;
- Data Origination Controls;
- Data Input Controls;
- Data Processing Controls;
- Data Output Controls;

b. The specific control techniques for each of these five components are detailed in this section. It should be noted that many techniques apply to more than one component; thus, this section should be referred to in its entirety to ensure coverage of all appropriate techniques.

2. System Design, Development, and Modification Controls.

The adequacy and effectiveness of controls in computer-based systems begins with the methods and procedures used during the system development process. Procedures should require a structured design, development, and modification process that provides adequate separation of duties and assures user, management, and internal auditor participation. Additional key elements are adequate documentation, effective computer program testing, effective system acceptance testing, and effective computer program change control procedures.

a. Systems Development Methodology Controls. Systems development should be predicated on life-cycle management (LCM) concepts and procedures. This technique is as applicable during initial system design as it is during the modification process; thus, appropriate elements of the LCM should be utilized whenever system changes are made. LCM is particularly advantageous because it promotes effective communication among programmers, systems analysts, acceptance testers, users, internal auditors, and management personnel.

The following techniques should be considered to properly control systems development:

(1) A formal management controlled approach for system development should exist;

(2) The system development process should include:

- Feasibility study.
- User need definition.
- Conceptual system design.
- Cost and/or benefit analysis.
- Detailed system analysis and design.
- Programming.
- Testing.
- Procedure preparation.
- Conversion.
- System acceptance.
- ADP Systems Security Office (ADPSSO) review and certification of protection specifications.
- Operations.
- Post-implementation audit.

(3) Formal requests for new or revised systems should be prepared by users submitted with proper authorization and used to develop the conceptual system design;

(4) The conceptual system design should be used to determine the technical and operational feasibility of the system;

(5) A cost and/or benefit analysis should be performed to ensure that the conceptual system will produce desired results economically;

(6) Additional hardware and system software requirements should be consistent with ADP plans and be included in the cost and/or benefit analysis, and be used to prepare the computer programs;

(7) The detailed system design should be consistent with the conceptual design, be based on the feasibility study and on the cost and/or benefit analysis, and be used to prepare the computer programs;

(8) Upon completion of all programming, each program, interrelated subsystem and the entire system should be thoroughly tested;

(9) Program and system test results should be reviewed and signed by the system analyst;

(10) Program and system test results should be reviewed by the ADP Systems Security Officer and certified that the system meets documented and approved system protection specifications;

(11) Procedures should exist to ensure that no data is lost or erroneously changed during conversion to the newly designed system;

(12) Sufficient computer time should be allocated for the conversion process;

(13) Prior to acceptance testing, the newly designed system should be tested in parallel operations with the old system;

(14) The system should be "acceptance tested" by a group independent of the programmers and analysts who designed the system to ensure that it performs in accordance with specifications and meets user needs;

(15) The system acceptance group should certify in writing that the system performs in accordance with all functional and performance specifications;

(16) This group should control all changes to the system to maintain its integrity on a continuing basis;

(17) System implementation should be coordinated with all personnel involved and other systems affected;

(18) A post-implementation audit of the entire system, manual and automated, should be performed by the internal audit staff after the system has been in operation for several months;

(19) The LCM concepts and procedures should be reviewed to assess whether they reflect current techniques and procedures applied in the ADP community;

(20) The following personnel should be involved in the system development process: project managers, users, system

analysts, programmers, records managers, acceptance testers and internal auditors;

(21) The duties of the personnel on the development project should be clearly separated;

(22) Specific tasks and timeframes for completing the tasks should be established for each member of the development project;

(23) The project manager should be authorized to make decisions on personnel resources, scheduling and most technical project matters;

(24) Adequate resources should be provided to successfully complete the system development project;

(25) A management project steering committee should be formed to oversee and review progress throughout the life-cycle;

(26) Users should actively participate in system development;

(27) The user should be the final authority on whether the system meets its intended purpose and should accept the system in writing.

b. System Reporting Documentation Controls. The objectives of documentation is to provide a clear, understandable description of the system. Good documentation increases the ease and accuracy of computer program maintenance and provides the basis for evaluating internal controls in the system. The following control techniques should be considered to ensure adequate system documentation:

(1) Ensure that programmers implement established standards for documenting different data processing functions;

(2) A project request document should be prepared to provide the means for a user to request the development, procurement, or modification of software or other ADP-related services;

(3) For significant system additions or modifications, a feasibility study document should be prepared to provide an analysis of the objectives, requirements and system concepts, an evaluation of alternative approaches, and an identification of a proposed approach;

(4) A cost and/or benefit analysis document should be prepared to give managers, users, designers, and auditors adequate information to evaluate alternative approaches for significant system additions or modifications;

(5) A functional requirements document should be prepared to provide the basic understanding between users and designers of the system;

(6) A data requirements document should be prepared to provide a data description and technical information about data collection requirements;

(7) Detailed system and/or subsystem specifications should be developed;

(8) Detailed program specifications should be developed for all programs of the system;

(9) Detailed specifications should be developed for data bases used by the system;

(10) A users or procedures manual should be developed to document the functions of the system;

(11) An operations manual should be developed to describe the system and its operational environment for computer operations personnel;

(12) Program and system documentation should be accessible to computer operations personnel;

(13) A program maintenance manual should be developed to give the maintenance programmer sufficient information to understand the programs, their operating environment, and their maintenance procedures;

(14) A plan should be documented to test the system;

(15) A test analysis report should be developed to document the test analysis results and findings;

(16) All documentation should be periodically reviewed to ensure that it is current and complete and adheres to established standards;

(17) Copies of all documentation should be stored off the premises;

(18) There should be signatures or other documented evidence of who performed systems and programming work;

(19) Documented procedures should exist for controlling all system documentation.

c. Program Testing and System Acceptance Controls

(1) Programs that make up a computer-based application should be thoroughly tested to assure accurate and reliable processing. Since programming errors can be made in either the symbolic language or program logic, error checking should be performed at several different stages in program development.

(2) The system acceptance process is the last line of defense against implementing an application with major errors. It serves as a "detective" control over the preceding phases of the development project. It gives users, internal auditors, designers, implementers, and other concerned parties an opportunity to view the system in final form before it becomes operational. If satisfied with results of the system acceptance process, acceptance testers should certify its accuracy and completeness in writing.

(3) The following control techniques should be considered to properly control program testing and system acceptance. It should be noted that current technology is addressing the automation of some of these controls.

(a) All computer programs should be checked by the programmer and his/her supervisor through desks checks or walk-throughs before program assembly or compilation;

(b) All computer programs should be reviewed after assembly or compilation to ensure that errors disclosed by these routines are corrected;

(c) Each program, subsystem, and then the entire system should be tested;

(d) Test data should be treated like live data, as opposed to entering codes in the test data to indicate that it is not normal production data.

(e) System acceptance should be performed using test data similar to, but independent of, program testing data;

(f) System acceptance transactions should be tested like live transactions, as opposed to having special codes entered in the transaction to indicate that it is not normal production data;

(g) Sufficient volumes of test and system acceptance transactions that have a wide range of valid and invalid conditions should be entered and processed;

(h) Sufficient time should be allocated for thorough testing and system acceptance purposes;

(i) Sufficient staff members should be allocated for testing and system acceptance purposes;

(j) Test cases and system acceptance test transactions should be developed to review:

- Mainline and end-of-job logic.
- Each routine.
- Each exception.
- Abnormal end-of-job conditions.
- Combinations of parameter cards and switch settings
- Unusual mixtures and sequences of data.
- Control features; e.g., salary parameters

(k) Test and system acceptance data should include cases that test for the following:

- Codes.
- Characters.
- Fields.
- Combination of fields.
- Transactions.
- Calculations.
- Missing data.
- Extraneous data.
- Amounts.
- Units.
- Composition.
- Logic decisions.
- Limit or reasonable checks.
- Sign.
- Record matches.

- Record mismatches.
- Sequence.
- Check digit.
- Crossfooting of quantitative data.
- Control totals.

(l) Programming and software packages should be used to improve computer programs' efficiency and effectiveness;

(m) New programs should be run parallel to old ones to help assure their accuracy;

(n) All computer-based systems should be subjected to a system acceptance process;

(o) The system acceptance should evaluate whether the entire system, both manual and automated processes, is performing in accordance with system specifications and processing standards;

(p) System acceptance should be performed by individuals independent of those who performed the analysis, design, and/or development of the system;

(q) Once system acceptance has been completed, a written certification that the entire system performs in accordance with all functional and performance specifications should be required before the system is placed in operation.

d. Program Change Controls. Control procedures for computer program changes should be established and followed. The intent of these controls is to prevent unauthorized, inaccurate, and unreliable program changes from being incorporated into the live production environment. Both scheduled and emergency changes need to be appropriately controlled to maintain the continued integrity of a computer-based system. The following control techniques should be considered to ensure that proper controls are being maintained over computer program changes:

(1) Formally approved written standards for program changes and documentation should exist and be followed;

(2) Procedures defining who can initiate and who can authorize change requests should be established;

(3) Change requests should be written, including a description of the nature of and reasons for the proposed change as well as security and privacy specifications;

(4) Change requests should be made by users on sequentially numbered forms;

(5) User authorization and written approval should be required for all program changes;

(6) ADP project management authorization and written approval should be required for all program changes;

(7) Changes should be approved by individuals who do not operate the computer, except for microcomputers;

(8) Procedures should exist to ensure that all program changes, both scheduled and emergency, are subjected to the testing and acceptance process;

(9) Application changes should be tested prior to operational use;

(10) Modified programs should be tested under normal operating conditions;

(11) Users should be involved in preparing test data and reviewing test results;

(12) Test results should be reviewed with supervisory personnel before revisions become effective;

(13) All errors detected during the conversion process should be investigated before and after correction;

(14) Certification should be made that test results demonstrate adequate protection from fraud, waste, and misuse of the program;

(15) All program changes should be documented, and appropriate program, system, operations, and user documentation should be updated as changes are made;

(16) A log should be maintained of all completed changes and all changes in progress;

(17) Program changes should be documented by individuals who do not operate the computer;

(18) Certification should be made that documentation specifications are met;

(19) Program library software should be used to report all changes to ADP managers and to users;

(20) Ensurances should be made that changes meet users' needs;

(21) Procedures should exist to determine if any other system if affected by the program modification;

(22) Original programs should be retained until changes have been processed and new programs tested and updated;

(23) Once modifications have been implemented, procedures should prevent original programs from being used by mistake;

(24) Procedures should be in place to ensure that an "abnormal" volume of regularly scheduled program modifications results in a review to determine if a problem exists with programs, procedures, or the computer-based system;

(25) A limit should be placed on the frequency of program changes, except for emergency changes;

(26) When emergency changes are made, both the user and ADP project manager should be notified;

(27) All problems related to program changes should be documented and given to the ADP project manager.

3. Data Origination Controls

a. Data origination controls are used to ensure the accuracy, completeness and timeliness of data prior to its being converted into machine-readable format and entered into the computer application. Controls over the data should be established as close to the point of origination as possible, as the remainder of the application processing depends upon the accuracy of source data. Additionally, controls should be maintained throughout this manual process to ensure that the data reaches the computer application without loss, unauthorized addition or modification, or other error.

b. The following control techniques should be considered to ensure that controls are being maintained over data origination:

(1) Documented procedures should exist to explain the methods for proper source document origination, authorization, data collection, input preparation, and error handling retention;

(2) Duties should be separated to ensure that no one individual performs more than one of the following: originating data, entering data, processing data, or distributing output;

(3) When beneficial, forms (either paper or electronic) may be used to record initial data in a uniform format;

(4) Source documents should be designed in such a manner as to minimize errors and omissions and to ensure data uniformity;

(5) Source documents should be prenumbered if accountability is a requirement;

(6) For each type of transaction, the source document should provide a unique identifying code;

(7) Each transaction should have a cross-reference number that can be used to trace data to and from the source document;

(8) Access to source documents, blank input forms and copies of source documents should be restricted to authorized personnel only;

(9) Authorizing signatures should be used for all paper transactions, when required;

(10) Duties should be separated within the user organization to ensure, unless authorized, that one individual does not prepare more than one type of transaction;

(11) Blank source documents should be stored in a secure location;

(12) Duties should be separated within the user organization to ensure that no one individual performs more than one of the following: originating the source document, authorizing the source document, or controlling the source document;

(13) The user organization should have a control group responsible for collecting and completing source documents;

(14) This control group should verify that source documents are complete and accurate. Furthermore, all documents should be accounted for, transmitted in a timely manner and authorized;

(15) A separate user group should perform the input function when the user organization is responsible for its own data entry;

(16) When transmitted for conversion, source documents should be transported in accordance with their security classifications;

(17) Documented procedures should exist to explain the methods for source document error detection, correction and reentry;

(18) The control group should identify errors to facilitate the timely correction of erroneous information;

(19) Error logs should be used to ensure timely follow-up and correction of unresolved errors;

(20) Originators of source documents should be notified by the control group of all error;

(21) Source documents should be retained as a safeguard against data loss or destruction during subsequent processing;

(22) Source documents should have specific retention periods;

(23) Source documents should be stored in a logical manner to facilitate retrieval;

(24) Whenever a source document leaves the originating organization, a copy should be kept in the organization;

(25) When reaching their expiration dates, source documents should be removed from storage and destroyed in accordance with the approved disposal schedule.

4. Data Input Controls

a. Data input controls ensure the accuracy, completeness and timeliness of data during its conversion into machine-readable format and entry into the application. Data can be entered through either on-line or batch processing. As there is a large degree of overlap between the control techniques for these two processes, no distinction is made in the following techniques indicating whether they apply to on-line, batch, or both.

b. The following control techniques should be considered to ensure that proper controls are being maintained over data input:

(1) Documented procedures should exist to explain the methods for data conversion and entry;

(2) Data entry terminal devices should be locked in a physically secure room;

(3) The work entered on a terminal should be restricted by the authority level assigned to each terminal;

(4) Password controls should be used to prevent unauthorized use of terminals;

(5) When keying passwords and authorization codes, non-printing and nondisplaying facilities should be used;

(6) An immediate report should be produced of unauthorized attempts to access the system via terminals;

(7) Management should review unauthorized usage reports;

(8) Each individual user of the on-line system should be limited to certain types of transactions;

(9) Individual passwords should be changed periodically;

(10) Passwords should be deleted once an individual changes his or her job function or level of access;

(11) Management should periodically review the propriety of the terminal authority levels;

(12) Terminal hardware features should include the following:

(a) Built-in terminal identifications that automatically validate proper terminal authorization,

(b) Terminal logs that are automatically data and time stamped for logging purposes, and

(c) Record counts that are automatically accumulated for logging purposes;

(13) Parity checking should be used to check each character and each message;

(14) Documented procedures should exist to explain the process of identifying, correcting and reprocessing data rejected by the application;

(15) Error messages should promptly be displayed with clearly understood corrective actions for each type of error;

(16) All data that does not meet edit requirements should be rejected from further processing by the application, produce an error message and be written on an automated suspense file;

(17) The suspense file should include the data and time a transaction was entered along with the identity of the user who originated the transaction;

(18) Suspense file processing should create record counts and predetermined control totals;

(19) Valid correction transaction should purge the automated suspense file of corresponding rejected transactions;

(20) All corrections should be reviewed and approved by supervisors before reentry;

(21) Procedures for processing corrected transactions should be the same as those for processing original transactions, except for the supervisory review and approval;

(22) The ultimate responsibility for the completeness and accuracy of all application processing should remain with the user;

(23) The terminal user should correct errors caused by data conversion or entry;

(24) The user originating the transaction should correct errors not caused by data conversion or entry;

(25) The suspense file should be used to control follow-up, correction, and reentry of rejected transactions;

(26) The suspense file should periodically be analyzed to determine whether too many errors are being made and whether corrections are being processed in a timely manner;

(27) Debit and/or credit entries, rather than delete or erase commands, should be used to correct errors on the suspense file;

(28) Record counts and predetermined control totals should be appropriately adjusted by correcting transactions;

(29) Intelligent" terminals should be used to allow front-end validation, editing, and control;

(30) Data validation and editing should be performed as early as possible in the data flow to ensure that the application rejects any incorrect transaction before its entry into the system;

(31) Preprogrammed keying formats should be used to make sure that data is recorded in the proper field, format, etc.;

(32) Computer-aided instruction, such as prompting, should be used with on-line dialogue to reduce the number of operator errors;

(33) Batch control totals, record counts, and predetermined control totals submitted by the data processing control group should be used by the computer-based system to validate the completeness of data input into the application;

(34) No personnel should be able to bypass validation and editing problems;

(35) Data validation and editing should be performed for all input data fields;

(36) All documents entered into the application should be signed or marked in some way to prevent accidental duplication or reuse of the data;

(37) The data processing organization should have a schedule by application showing when data requiring conversion and when data requiring entry will be received and needs to be completed;

(38) Input document should be retained in a manner that enables tracing them to related originating documents and output records;

(39) All converted documents and input documents returned to the data processing control group should be logged in and accounted for;

(40) The data processing organization should have a control group responsible for data conversion and entry of all source documents received from users;

(41) This group should account for all batches of source documents received from the user to ensure that no batches have been added or lost;

(42) This group should independently develop record counts and predetermined control totals to be balanced with those of the control group in the user organization, and all discrepancies should be reconciled.

5. Data Processing Controls

a. Data processing controls are used to ensure the accuracy, completeness, and timeliness of data during processing

by the computer. These controls apply to application programs and computer operations related to a given application. Data processing is usually accomplished in either batch or real time. As with data input controls, no distinction is made in the listing of the data processing control techniques for batch versus real time.

b. The following techniques should be considered to ensure that proper controls are being maintained over data processing. Several of the techniques listed previously in this section, particularly those relating to editing and error handling, are applicable to data processing as well. The reader should refer back as the following techniques are considered:

(1) Documented procedures should exist to explain the methods for proper data processing of each application program;

(2) Operator instructions should include system start-up procedures, backup assignments, emergency procedures, system shutdown procedures, error message debugging instructions and system and job status reporting instructions;

(3) Application programs should be prevented from accepting data from computer consoles;

(4) The system should have a history log that is printed on both a line printer and the console;

(5) The log should routinely be reviewed by supervisors to determine the cause of problems and the appropriateness of actions taken;

(6) The data processing organization should have a schedule showing when each application program is to be run and needs to be completed;

(7) The data processing organization should have a control group responsible for controlling all data processing operations;

(8) Each input transaction should have a unique identifying transaction code that directs it to the proper application program for processing;

(9) Standardized default options should be built into the program logic;

(10) Computer generated control totals (run-to-run totals) should automatically be reconciled to check for completeness of processing;

(11) Controls should be in place to prevent operator from circumventing file checking routines;

(12) Controls should ensure that output counts equal input counts;

(13) All programs that include a table of values should have an associated control mechanism to ensure accuracy of the table value;

(14) There should be an audit trail in the application to assist in reconstructing data files;

(15) Messages and data should be able to be traced back to the user or to the point of origin;

(16) The application should prevent concurrent file updates;

(17) Transactions should be dated and time-stamped for logging purposes;

(18) There should be control to verify that proper data is used when computerized data is entered into the computer application;

(19) When computerized files are entered into the computer application, there should be controls to verify that the proper version of the file is used;

(20) Application programs should include routines for checking internal file header labels before processing;

(21) Internal trailer labels should contain control totals to provide a check that all records are on the file;

(22) File completion checks should be performed to ensure that application files have been completely processed, including both transaction and master files;

(23) Record and predetermined control totals generated by the application should be used by the data processing control group to validate the completeness of data processed by the system;

(24) A direct update to files should cause creation of a record added to a backup file and recording of the transaction on the transaction history file;

(25) A "before and after picture" of the master file being updated should be maintained;

(26) Relationship editing should be performed between the input transaction and master files to check for appropriateness and corrections prior to updating;

(27) The data processing control group should balance batch counts, record counts, and predetermined control totals of data submitted for processing; ensure that input and/or work and/or output files used in computer processing are correct and maintained in logs; and ensure that restarts are properly performed.

6. Data Output Controls. Data output controls are used to ensure the integrity of output and the correct and timely distribution of outputs produced. Not only must outputs be accurate, but they must also be received by users in a timely and consistent manner. Of critical importance is the interface between the data processing organization and the user department. Outputs can be produced either in a batch mode or on-line. Again, as there is a large degree of overlap in the control techniques for these two methods, no distinction is made within the specific techniques.

a. Documented procedures should exist to explain the methods for proper balancing and reconciliation of output products;

b. The data processing organization should have a control group that is responsible for reviewing all outputs produced by the application;

c. This group should monitor the processing flow to ensure that programs are process according to schedule;

d. This group should review output products for general acceptability and completeness;

e. This group should reconcile each output batch total, record count and predetermined control total with input batch totals, record counts and predetermined control totals before releasing any reports in order to ensure that no data was added or lost during processing;

f. System output logs should be kept to provide an audit trail for the outputs and to summarize the number of reports generated, the number of copies of each report, the recipients of each report and the report security status;

g. These logs should be reviewed by supervisors to determine the correctness of output production;

h. A transaction log kept by the application should be compared regularly with a transmission log kept at each output device to ensure that all transactions have been properly processed to the final output steps;

i. Transactions should be able to be traced forward to the final outputs and backward to the original source documents;

j. The user should have a control group that is responsible for reviewing all output received from the data processing organization;

k. This group should be given lists of all changes to the application master file data and programmed data, of all internally generated transactions produced by the application, of all interface transactions processed by the application, and of all transactions entered into the application;

l. This group should use these lists to verify the accuracy and completeness of all output;

m. This group should verify all computer-generated batch totals, record counts and predetermined control totals with its own manually developed batch totals, record counts, and predetermined control totals;

n. Documented procedures should exist to explain the methods for proper handling and distribution of output reports;

o. Users should periodically be questioned to determine whether they find the reports they receive relevant; whether they find the data presented on reports accurate, reliable and useful; whether they should be removed form or added to distribution lists for receiving reports; and whether they have suggestions concerning the format, content, frequency, and timeliness of reports they receive;

p. The user should retain ultimate responsibility for the accuracy of all outputs;

q. The cover sheet of every report should clearly identify the recipients' names and locations;

r. A priority system should exist to ensure that critical outputs are produced on time;

E. MICROCOMPUTER CONTROLS. Control procedures over microcomputer acquisition and operation should be established and followed to ensure the proper use of microcomputers and the accuracy of the processed data. Implementing certain control procedures unique to microcomputers should decrease the risk of illegal system access, data loss, and stolen hardware. Internal control techniques enumerated elsewhere in this Guideline may also apply to microcomputer. The reader should refer to the techniques detailed under Management Controls, Operations Controls, and Application Controls to ensure control over microcomputer operation. The following techniques should be considered to ensure that proper controls exist in the microcomputer environment:

1. ADP and user management should establish and document microcomputer acquisition policies, criteria, and procedures within an approved organizational statement of strategy;

2. Acquisition should be justified in terms of objectives and benefits to be realized, and the level of detail in the justification documentation should be kept to a minimum, commensurate with need and judicious management practices;

3. Management should be established allowing only authorized personnel use of microcomputer resources to protect the data, software, and physical equipment from improper use or theft;

4. Policies should be established allowing only authorized personnel use of microcomputer resources to protect the data, software, and physical equipment from improper use or theft;

5. Requisition, approval, and subsequent placement of microcomputers should be documented;

6. Written guidelines should exist on develop-or-buy alternatives for application software;

7. Personnel with appropriate backgrounds should be designated to develop application software and/or to evaluate application software packages offered by vendors.

8. Procedures should exist to allow user groups to accept application software developed internally;

9. User groups should be required to provide program documentation for approval prior to using application software developed by the group;

10. Management approval and user group concurrence should be secured in instances when data processing personnel modify application software packages;

11. Management approval should be secured before application software packages are modified by user groups;

12. A procedures manual should be developed to document the functions and capabilities of microcomputer-based systems;

13. Procedures related to sharing application programs and data should be established;

14. A central depository of documentation of programs under development should be kept to prevent duplication of effort;

15. Proprietary software packages should be protected against copying or modification;

16. A formal document should state that copyright laws will be rigidly enforced;

17. Hard disks should be backed up onto another storage medium on a regular basis;

18. When microcomputers are approved to access data in other computer facilities, procedures that adhere to policy concerning the creation and maintenance of data files on these microcomputers would be specified;

19. When microcomputers are approved to access data in other computer facilities, procedures that adhere to policy concerning gaining access to microcomputers and other computer resources accessible to these microcomputers should be established;

20. Codes, passwords, or other devices should be used to identify authorized users of the microcomputers;

21. When microcomputers are approved to access data in the organization's other computer facilities, usage on these microcomputers, including user identification, level of resource access, and all transactions introduced for processing should be logged by the other facilities;

22. When they are away from the microcomputer area, users of sensitive data should securely lock up all diskettes;

23. Rooms in which microcomputers are located should be secured after normal working hours;

24. Microcomputers should be stored in a controlled area;

25. Property management procedures concerning microcomputer components should be followed, including marking them with unique identification numbers and recording and securely storing all identification numbers, serial numbers, and equipment descriptions.

APPENDIX

Life-Cycle Management-

Internal Control

Techniques

This is the first attempt to integrate control techniques with the life-cycle phases. The results indicate there is room for refinement and identification of additional control techniques, especially in the early phases.

The items shown in bold (and solid bullet), below, identify those tasks and products that are required for each LCM Phase of an AIS project. AIS internal control techniques to be considered when developing those tasks or products are included (not in bold) under the appropriate LCM bullets. The AIS internal control techniques are from Chapter 6.

A. **Need Justification (Phase 0)**

1. • **Identification of Mission Deficiency.**

o **Functional or Operational.**

a. AIS Planning

(1) An AIS management process that considers inputs from the various involved organizations, including major user departments and program areas, should be applied to justify the need for new automated equipment.

(2) The planning process should establish and document mission requirements, strategy, and overall system goals and objectives.

2. • **Conduct Analyses.**

o Security or other vulnerability analyses.

o Characterizing the current and projected environment to include wartime role, if any.

o Estimated Time And Cost for Corrective Action (level of effort).

o Standardization, Integration, and Interface Requirements.

a. AIS Planning

(1) An AIS management process that considers inputs from the various involved organizations, including major user departments and program areas, should be applied to ensure that new equipment is acquired in the most economical and expeditious manner.

(2) AIS planning should be related to budgeting for financial, personnel, and system resources.

(3) The AIS planning process should take into account relevant computer security requirements affecting the scope of ADP activity.

b. Policies, Standards, and Procedures

(1) Policy and procedures should be established to comply with systems security, privacy, and freedom of information requirements.

c. Internal Audit

(1) Internal Audit should actively participate in reviewing the development of new systems or applications and the significant modification of existing systems.

d. Distributed Processing and Network Operations Controls

(1) The operating provisions in the implementation plan should be consistent with the laws and regulations governing transmission of data within the country and/or internationally.

3. • **Information Reporting Requirements Approved in Accordance with DoD Directive 7750.5 (reference (p)).**

a. AIS Planning

(1) The AIS planning process should establish and document individual responsibility for specific actions to be undertaken.

b. System Reporting Documentation Controls

(1) A functional requirements document should be prepared to provide the basic understanding between users and designers of the system.

(2) A data requirements document should be prepared to provide a data description and technical information about data collection requirements.

4. • **Preparation of Mission Need Statement (MNS).**

a. AIS Planning

(1) The planning process should establish and document mission requirements, strategy, and overall system goals and objectives.

b. Systems Development Methodology Controls

(1) The system development process should include user need definition.

5. • **Submission of MNS to LCM review and milestone approval authority.**

a. Policies, Standards, and Procedures

(1) Rigorous AIS budgeting procedures should be implemented to ensure that all significantly ADP-related initiatives, expenditures, and reprogramming are clearly highlighted, whether or not they fall within budget decision units or are spread over multiple decision units.

b. Systems Development Methodology Controls

(1) Formal requests for new or revised systems should be prepared by users submitted with proper authorization and used to develop the conceptual system design.

c. System Reporting Documentation Controls

(1) A project request document should be prepared to provide the means for a user to request the development, procurement, or modification of software or other AIS-related services.

B. Concepts Development (Phase 1)

1. • **Mission Need Reaffirmed.**

2. • **Project Manager Appointed and Chartered.**

a. AIS Planning

(1) The AIS planning process should establish and document individual responsibility for specific actions to be undertaken.

b. System Development Methodology Controls

(1) A formal management controlled approach for system development should exist.

(2) The project manager should be authorized to make decisions on personnel resources, scheduling, and most technical project matters.

(3) A management project steering committee should be formed to oversee and review progress throughout the life cycle.

3. • **Functional Objectives Prioritized.**

a. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

(2) Rigorous project control and performance measurement techniques (e.g., PERT, CPM) and progress reporting should be required based upon actual cost and work-year expenditures, deliverables provided, and milestones achieved (rather than upon subjective percent of completion estimates).

b. Distributed Processing and Network Operations Controls

(1) A central control function should be established to coordinate control reviews of network assets and resources at all network locations.

(2) Network output requirements, operating schedules, processing procedures and facility coordination policies should be fully established.

(3) Policy agreements should exist for communications transmissions, including provisions to effectively interface software applications and data bases among coordinated network facilities.

c. Systems Development Methodology Controls

(1) The system development process should include user need definition.

(2) Procedures should exist to ensure that no data is lost or erroneously changed during conversion to the newly designed system.

(3) Users should actively participate in system development.

d. Data Input Controls

(1) Data validation and editing should be performed as early as possible in the data flow to insure that the

application rejects any incorrect transaction before its entry into the system.

4. • **Develop Functional Descriptions.**

a. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

b. Distributed Processing and Network Operations Controls

(1) Policy agreements should exist for communications transmissions, including provisions to effectively interface software applications and data bases among coordinated network facilities.

c. Systems Development Methodology Controls

(1) Users should actively participate in system development.

d. System Reporting Documentation Controls

(1) A data requirements document should be prepared to provide a data description and technical information about data collection requirements.

5. • **Demonstrate Feasible Alternatives.**

a. AIS Planning

(1) AIS planning should be related to comparing and selecting among system alternatives based upon quantified life-cycle cost, benefit, and risk projections.

b. Systems Development Methodology Controls

(1) The conceptual system design should be used to determine the technical and operational feasibility of the system.

c. System Reporting Documentation Controls

(1) A cost-benefit analysis document should be prepared to give managers, users, designers, and auditors adequate information to evaluate alternative approaches for significant system additions or modifications.

6. • **Update Cost and Time Estimates.**

a. AIS Planning

(1) An AIS management process that considers inputs from the various involved organizations, including major user departments and program areas, should be applied to ensure that new equipment is acquired in the most economical and expeditious manner.

(2) AIS planning should be related to budgeting for financial, personnel, and system resources.

b. Systems Development Methodology Controls

(1) Specific tasks and timeframes for completing the tasks should be established for each member of the development project.

c. System Reporting Documentation Controls

(1) A cost and/or benefit analysis document should be prepared to give managers, users, designers, and auditors adequate information to evaluate alternative approaches for significant system additions or modifications.

7. • **Preliminary Planning (Training, Log).**

a. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

b. Policies, Standards, and Procedures

(1) All appropriate organizational components of the site involved with ADP systems should be defined and clearly assigned their respective areas of functional responsibility.

(2) Procedures describing the manner and responsibility for performance between users and ADP should be established, coordinated, and communicated to all affected organizations.

c. Organizational Controls

(1) The ADP function should be placed sufficiently high in the organization to ensure its independence from other site operations.

(2) Major organizational units within ADP should be described and their responsibilities delineated and documented.

(3) Training programs should exist to maintain and build skills, knowledge, and ability in systems technology as well as internal control and ADP security requirements.

d. Workload Scheduling Controls

(1) Formal input and/or output control procedures should be established and documented.

(2) The control group should establish and document formal scheduling procedures, schedule production runs and other workloads, and reschedule aborted or erroneous processing.

e. Malfunction Reporting and Preventive Maintenance Controls

(1) Formal malfunction reporting procedures should be established and documented for the data processing installation.

f. User Billing and Charge-back Controls

(1) Procedures for user billing and charge should be documented.

g. Distributed Processing and Network Operations Controls

(1) The distributed processing requirements definitions should be responsive to management objectives in terms of the hardware configuration, data base configuration and hardware, and communications network interface.

(2) The operating provisions in the implementation plan should be consistent with the laws and regulations governing transmission of data within the country and/or internationally.

(3) Network data policies should require that data set ownership be clearly established.

(4) Policy agreements should exist for communications transmissions including provisions to effectively interface software applications and data bases among coordinated network facilities.

h. Data Origination Controls

i. Data Input Controls

j. Data Processing Controls

k. Data Output Controls

1. Microcomputer Controls

8. • **Develop Acquisition Strategy.**

9. • **Standardization and Interoperability.**

a. Distributed Processing and Network Operations Controls

(1) The operating provisions in the implementation plan should be consistent with the laws and regulations governing transmission of data within the country and/or internationally.

(2) Appropriate techniques and policies should be instituted for standardizing data definitions of shared data, maintaining common data dictionaries, and reconciling deviations in data definition at remote facilities.

10. • **Areas of Risk and Uncertainty Identified.**

a. Internal Audit

(1) The responsibility of the internal audit function in relation to ADP should be clearly documented.

b. Administrative Controls

(1) Responsibility for conducting risk analyses should be formally assigned.

(2) Risk analysis studies should measure vulnerability related to the potential for the following:

(a) Fraud or theft,

(b) Inadvertent error or improper disclosure of information,

(c) Financial loss,

(d) Harm to individuals or infringement on privacy rights,

(e) Loss of proprietary data and harm to organizational activities.

(3) A Specific timetable for conducting risk analysis studies should be established, with the time between studies being comMNSurate with the sensitivity of the information processed.

(4) Procedures should require that a risk analysis be performed before the approval of design specifications for computer installations or whenever significant changes are made

to the physical facility, hardware, or operating system software.

11. • **Develop AIS Transition Strategy.**

12. • **Establish Configuration Management Discipline.**

a. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

13. • **Electronic Countermeasure Requirements.**

14. • **Plan for Preparation of T&E Plan.**

a. Policies, Standards, and Procedures

(1) Rigorous project control and performance measurement techniques (e.g., PERT, CPM) and progress reporting should be required based upon actual cost and work-year expenditures, deliverables provided, and milestones achieved (rather than upon subjective percent of completion estimates).

15. • **Communications Requirements.**

16. • **Privacy and Security Requirements.**

a. AIS Planning

(1) The AIS planning process should take into account relevant computer security requirements affecting the scope of ADP activity.

17. • **Contractor vs. In-House Analysis.**

a. AIS Planning

(1) An AIS management process that considers inputs from the various involved organizations, including major user departments and program areas, should be applied to assure that new equipment is acquired in the most economical and expeditious manner.

(2) AIS planning should be related to comparing and selecting among system alternatives based upon quantified life cycle cost, benefit, and risk projections.

18. • **Preparation of System Decision Paper (SDP-1).**

19. • **Submit SDP to LCM review and milestone approval authority.**

a. AIS Planning

(1) AIS planning should be related to comparing and selecting among system alternatives based upon quantified life-cycle cost, benefit, and risk projections. A full cost benefits analysis is not expected until Milestone II.

(2) The planning process should measure and compare actual accomplishments with expected performance throughout the system life cycle.

b. Systems Development Methodology Controls

(1) A formal management controlled approach for system development should exist.

(2) The system development process should include conceptual system design.

(3) Formal requests for new or revised systems should be prepared by users submitted with proper authorization and used to develop the conceptual system design.

(4) The conceptual system design should be used to determine the technical and operational feasibility of the system.

C. **Design (Phase 2)**

1. • **Mission Need Reaffirmed.**

a. AIS Planning

(1) Regular internal audit review and reporting should be conducted regarding completed and proposed planning decisions in relation to mission requirements.

2. • **Functional System Design Revalidated.**

o Baseline Updated.

a. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

b. Systems Development Methodology Controls

(1) The conceptual system design should be used to determine the technical and operational feasibility of the system.

3. • **Develop AIS Specifications for hardware, software and databases.**

a. Data Origination Controls

(1) Special forms should be used to guide the initial recording of data in a uniform format.

(2) Source documents should be designed in such a manner as to minimize errors and omissions and to ensure data uniformity.

(3) Source documents should be pre-numbered, if appropriate.

(4) For each type of transaction, the source document should provide a unique identifying code.

(5) Each transaction should have a cross-reference number that can be used to trace data to and from the source document.

b. Policies, Standards, and Procedures

(1) AIS resources acquisition, system design, programming, and operating standards should be established, coordinated, and communicated to all affected personnel.

c. Technical Controls

(1) Separate security software should be used to provide control over the site's computer resource.

(2) The security software should control access to terminals, remote job entry station, individual automated data files, application programs, and other system software;

(3) Security software functions should be adequately supported by proper manual procedures.

(4) The vendor or developer of the security software should provide a completely documented description of its design and operation.

(5) The control functions performed by security software should not be able to be overridden or bypassed.

(6) The security software should provide an audit trail of all authorized uses and unauthorized attempted accesses of computer resources under control.

(7) The security software should control access to data in a different manner than access to other computer resources.

(8) The security software should be transparent to all application programs and to all other system software.

(9) In an on-line environment, there should be access security control based on the classification of file data and devices.

(10) Sensitive files, such as security classifications or Privacy Act restrictions, should be properly identified as such, and appropriately secured.

d. Operating Systems Controls

(1) The operating system should prohibit one application program from accessing memory or data of another application program that is processing simultaneously.

(2) The use of privileged instruction of the operating system should be strictly controlled.

(3) The operating system should prohibit an application program from accessing operating system instructions, password tables and other security algorithms.

(4) The operating system should prohibit operators from entering application data or changing users' memory values at the computer console.

(5) The operating system should control all input and or output functions of data files.

(6) Operating system instructions, password tables, and other authorization algorithms should be protected from unauthorized access when the computer system fails.

(7) Provisions should be made to prohibit application programs from overriding or bypassing errors that are detected during processing.

(8) All application programs or other system software should be run only when the operating system is operational.

(9) An audit trail of all operating system actions should be maintained either on the automatic console log or as part of the computer system's job accounting data.

(10) The computer system's internal clock should be adequately protected from unauthorized access.

(11) The operating system should adequately and accurately schedule all jobs run on the computer system.

e. System Utilities Controls

(1) Controls that detect processing errors in system utilities should not be able to be overridden or bypassed.

(2) System utilities should not be able to be used to override or bypass controls within other system software or application programs.

f. Program Library Systems Controls

(1) A program library system should be used to control application programs.

(2) The program library system should restrict access to application programs, control movement of programs from test to production modes, control movement of programs from source code to object code, and control changes to application programs.

(3) Control functions performed by the program library system should be protected so they cannot be bypassed.

(4) The program library system should provide an audit trail of all changes made to application programs.

(5) The program library system should prevent the existence of more than one version of a source code and object code program.

g. File Maintenance Systems Controls

(1) A file maintenance system should be used to control all disk and tape data set.

(2) The file maintenance system should control the establishment, use, and retention of automated data files.

(3) Functions of the data communications system should be protected so that they cannot be overridden or bypassed.

(4) A built-in hardware identification code should be checked by the data communications system to ensure that no unauthorized terminals are being used.

(5) The data communications system should use a table of authorized terminal addresses to allow polling with the communications network.

(6) Control functions performed by the file maintenance system should be protected so that they cannot be overriden or bypassed.

(7) The file maintenance system should include redundancy controls such as prohibiting more than one data file from having the same volume serial number.

(8) User authorization codes or passwords should be required by the data communications system to access the computer system and application programs, other system software and to enter transactions.

(9) Different authorization codes should be required to enter different types of transactions.

(10) The authorization code should identify the individual using the terminal and should be periodically changed.

(11) A nonprinting and/or nondisplaying facility should be used when keying in and acknowledging user authorization codes.

(12) A terminal identification check should be performed by the data communications system so that various transaction types can be limited to authorized data entry stations.

(13) The security matrix or table used to control access to the application system should be properly protected to prevent unauthorized access.

h. Data Communications Systems Controls

(1) A data communications system should serve as the interface between terminals and the central data processing system.

(2) Functions of the data communications system should be protected so that they cannot be overridden or bypassed.

(3) The data communications system should control access to and use of terminals, poll and receive messages from computer terminals or other computers, address and send messages back to computer terminals or other computers, edit and format input and output messages, handle error situations, reroute traffic when terminals or lines are inoperative, and perform on-line formatting on visual display terminals.

(4) A built-in hardware identification code should be checked by the data communications system to ensure that no unauthorized terminals are being used.

(5) The data communications system should use a table of authorized terminal addresses to allow polling with the communications network.

(6) User authorization codes or passwords should be required by the data communications system to access the computer system and application programs, other system software, and to enter transactions.

(7) Different authorization codes should be required to enter different types of transactions.

(8) The authorization code should identify the individual using the terminal and should be periodically changed.

(9) A nonprinting and/or nondisplaying facility should be used when keying in and acknowledging user authorization codes.

(10) A terminal identification check should be performed by the data communications system so that various transaction types can be limited to authorized data entry stations.

(11) The security matrix or table used to control access to the application system should be properly protected to prevent unauthorized access.

(12) A message header should be used by the data communications system to identify the source of the message, including proper terminal and use authorization code, message sequence number, including total number of message segments, transportation type code, and transportation authorization code.

(13) This message header should be validated by the data communications system for proper sequence number from the identified terminal, proper transaction code and /or user authorization code for the terminal or user, and number of message segments received equal to the count indicated in the message header, proper acknowledgment from the terminal at the end of a transmission, and balancing of debit and/or credit totals derived from adding all message segments and comparing them with corresponding totals in the message header.

(14) The data communications system should include an end-of-transmission trailer that includes message and segment, value totals, including debits and credits, if appropriate, and an ending symbol.

(15) The data communications systems should reconcile counts and totals with header counts and totals.

(16) The data communications system should send acknowledgments to the terminal indicating receipt of messages and periodically test line and terminal operating status with standardized test messages and responses.

(17) The data communications system should use buffering to queue messages when a device, such as a terminal, is busy.

(18) The data communications system should maintain a transaction log of sequentially numbered and/or time-of-day-noted transactions.

(19) The transaction log should record the originating terminal, user authorization code, message identification, transaction type code, time of day that the transaction was logged, and transaction data.

(20) The transaction log should provide part of the audit trail, account for all error messages, and record, with control totals, all retrievals made by a particular terminal.

(21) All messages awaiting transmissions should be logged by the data communications system before being put into the transmission queue and then purged after successful transmission.

i. System Software Change Controls

(1) Formal documented system software change procedures should be established.

(2) Procedures should be established so that the accepted emergency modifications will be incorporated into the next operational version of the system software.

(3) Procedures should be established to ensure that emergency system software modifications are immediately subjected to a system acceptance test.

j. Data Base Management Systems Controls

(1) Where appropriate, responsibility for administering the data base environment should be established at a high enough level to ensure independence.

(2) The vendor or developer of the data base management system should provide a complete documented description of its design and operation.

(3) The data base management system should provide security over data base accesses, control the addition, modification, and deletion of data, and provide a complete documented description of its design and operation.

(4) Integrity of data maintained within the data base should be ensured through utility programs that check the physical linkage of data within the database, control records

that maintain interim balances of transactions and apply application programming standards that include procedures for maintaining integrity.

(5) Data base management system functions should be adequately supported by proper manual procedures.

(6) Functions of the data base management system should be protected so that they cannot be overridden or bypassed.

(7) The use of restricted instructions should be logged and checked periodically.

(8) The data base management system should use authorization codes or passwords to control access to data items.

(9) The data base management system should record unsuccessful attempts to access the data base.

(10) The data base management system should record which application programs have accessed each data item within the data base.

(11) The data base management system should prevent simultaneous updates to a record.

(12) The data base management system should prevent shared data from being deleted without consent of all users of the data.

(13) A log should indicate whether an application program has read, updated, created, or deleted a data item.

(14) All errors discovered by the data base management system should be logged for follow-up.

(15) Failures in the data base management system should be documented for supervisory review.

(16) A data dictionary should be developed and maintained, documenting the attributes of each data item and the security over each data item.

k. Central Processing Unit Controls

(1) Built-in parity bits should be used by the CPU to ensure that all data elements transmitted through the internal circuitry are correctly transmitted.

(2) Redundant character checking should be used by the CPU to ensure the correctness of data processing.

(3) The CPU should use validity checks to ensure that only valid operation codes are used.

(4) The CPU should perform validity checks on the numbers used to access memory to ensure that only valid numbers are used.

(5) The CPU should have automatic interlock controls to prevent the equipment from performing certain operations at the wrong time.

(6) Log should be maintained to record CPU meter readings at the start and end of each shift, and variances should be explained.

1. Peripherals Controls

(1) Parity checks of both individual and blocks of data should be made to ensure that all data elements are transmitted accurately.

(2) Validity check controls should be used to check the results of an operation with all possible valid solutions.

(3) Echo checks should be used to ensure that a transmitted command is actually performed or the data sent is correct.

(4) A read-after-write check should be used to ensure that the record just written was correctly recorded.

(5) Equipment diagnostic tests should exist for the computer to check if the equipment is functioning properly.

(6) With direct access storage devices, address comparisons should be made to verify the address to which data is to be written with the address called for by the instruction.

(7) Print synchronization controls should be used to check the timing of the printer to determine that print hammers of impact printers are activated at the moment when appropriate characters are in the correct position.

4. • **Communications Requirements.**

a. Distributed Processing and Network Operations Controls

(1) Hardware controls should include memory protection, alternate communication routing, communication protocols, and timely failure recovery mechanisms;

(2) Software controls over reentrant operating systems and current data base accesses and update should exist.

(3) Commonly shared and distributed data should be designed to readily permit integration and summarization at an organization-wide level to meet current or anticipated objectives.

(4) Adequate disaster and recovery procedures should be developed for each network processing facility. These procedures should be current and periodically tested.

(5) Network data standards should require and define data set change control procedures.

(6) Standards and policies for general network control should be clearly established and followed.

(7) Network standards and policies should be sufficiently broad-based, not to encumber local autonomy or operating objectives.

(8) As the general network capability is distributed, controls should be distributed to users.

(9) A network policy should require the ongoing identification of data set needing inter-system compatibility.

(10) A network should exist requiring audit trails and backup of all network communications activity for both network messages and application processed data.

(11) A network implementation, conversion and acceptance plan should be developed jointly by systems and network user organizations and include user-prescribed test procedures and acceptance criteria.

(12) User and system responsibilities should be fully defined for coordinating and reconciling differences between distributed and/or replicated data bases prior to network implementation.

(13) Reconciliations should be able to be satisfactory performed under normal conditions, following network failures, and between varying application problems.

(14) Each network message and/or transmitted data unit should contain codes that identify the sender and intended receiver(s).

(15) All changes made to network operating systems software at remote processing facilities should be controlled by the central and/or main network processing facilities.

(16) A network data review mechanism should be established to administer compatibility between system and data as the network grows.

b. Systems Development Methodology Controls

(1) The system development process should include detailed system analysis and design.

(2) Planning for the new facility to include reliable power, (UPS), communications lines, air conditioning, raised floors, (if applicable), fire protection equipment.

(3) Additional hardware and system software requirements should be consistent with ADP plans and be included in the cost and/or benefit analysis, and be used to prepare the computer programs.

(4) Users should actively participate in system development.

(5) The detailed system design should be consistent with the conceptual design, be based on the feasibility study and on the cost-benefit analysis, and be used to prepare the computer programs.

c. System Reporting Documentation Controls

(1) Detailed system and/or subsystem specifications should be developed.

(2) Detailed program specifications should be developed for all programs of the system.

(3) Detailed specifications should be developed for data bases used by the system.

d. Data Origination Controls

(1) Duties should be separated to ensure, unless authorized, that no one individual performs more than one of the following: originating data, entering data, processing data, or distributing output.

(2) Access to source documents, blank input forms, and copies of source documents should be restricted to authorized personnel only.

(3) Authorizing signatures should be used for all paper transactions, when required.

(4) Duties should be separated within the user organization to ensure, unless authorized, that one individual does not prepare more than one type of transaction.

(5) Duties should be separated within the user organization to ensure, unless authorized, that no one individual performs more than one of the following: originating the source document, authorizing the source document, or controlling the source document.

(6) The user organization should have a control group responsible for collecting and completing source documents.

(7) This control group should verify that source documents are complete and accurate. Furthermore, all documents should be accounted for, be transmitted in a timely manner, and have been appropriately authorized.

(8) A separate user group should perform the input function when the user organization is responsible for its own data entry.

(9) The control group should identify errors to facilitate the timely correction of erroneous information.

(10) Error logs should be used to ensure timely follow-up and correction of unresolved errors.

(11) Originators of source documents should be notified by the control group of all errors.

e. Data Input Controls

(1) Password controls should be used to prevent unauthorized use of terminals.

(2) When keying passwords and authorization codes, nonprinting and nondisplaying facilities should be used.

(3) An immediate report should be produced of unauthorized attempts to access the system via terminals.

(4) Terminal hardware features should include the following:

(a) Built-in terminal identifications that automatically validate proper terminal authorization.

(b) Terminal logs that record all transactions processed.

(c) Record counts that are automatically accumulated for logging purposes.

(5) Parity checking should be used to check each character and each message.

(6) Error messages should promptly be displayed with clearly understood corrective actions for each type of error.

(7) All data that does not meet edit requirements should be rejected from further processing by the application, produce an error message, and be written on an automated suspense file.

(8) The suspense file should include the date and time a transaction was entered along with the identity of the user who originated the transaction.

(9) Suspense file processing should create record counts and predetermined control totals.

(10) Valid correction transaction should purge the automated suspense file of corresponding rejected transactions.

(11) The suspense file should be used to control follow-up, correction and reentry of rejected transactions.

(12) Debit and/or credit entries, rather than delete or erase commands, should be used to correct errors on the suspense file.

(13) Record counts and predetermined control totals should be appropriately adjusted by correcting transactions.

(14) "Intelligent" terminals should be used to allow front-end validation, editing and control.

(15) Data validation and editing should be performed as early as possible in the data flow to ensure that the application rejects any incorrect transaction before its entry into the system.

(16) Preprogrammed keying formats should be used to make sure that data is recorded in the proper field, format.

(17) Computer-aided instruction, such as prompting, should be used with on-line dialog to reduce the number of operator errors.

(18) Batch control totals, record counts, and predetermined control totals submitted by the data processing control group should be used by the computer-based system to validate the completeness of data input into the application.

(19) Data validation and editing should be performed for all input data fields.

(20) Input document should be retained in a manner that enables tracing them to related originating documents and output records.

(21) All converted documents and input documents returned to the data processing control group should be logged in and accounted for.

(22) Procedures for processing corrected transactions should be the same as those for processing original transactions, except for the supervisory review and approval.

(23) The ultimate responsibility for the completeness and accuracy of all application processing should remain with the user.

(24) The terminal user should correct errors caused by data conversion or entry.

(25) The user originating the transaction should correct errors not caused by data conversion or entry.

(26) All documents entered into the application should be signed or marked in some way to prevent accidental duplication or reuse of the data.

(27) The data processing organization should have a control group responsible for data conversion and entry of all source documents received from users.

(28) With proper password protection, personnel should not be able to bypass validation and editing problems.

f. Data Processing Controls

(1) The data processing organization should have a control group responsible for controlling all data processing operations.

(2) Application programs should be prevented from accepting data from computer consoles.

(3) The system should have a history log that is printed on both a line printer and the console.

(4) Each input transaction should have a unique identifying transaction code that directs it to the proper application program for processing.

(5) Standardized default options should be built into the program logic.

(6) Computer-generated control totals (run-to-run totals) should automatically be reconciled to check for completeness of processing.

(7) Controls should be in place to prevent operator from circumventing file checking routines.

(8) Controls should ensure that output counts equal input counts.

(9) All programs that include a table of values should have an associated control mechanism to ensure accuracy of the table value.

(10) There should be an audit trail in the application to assist in reconstructing data files.

(11) Messages and data should be able to be traced back to the user or to the point of origin.

(12) The application should prevent concurrent file updates.

(13) Transactions should be date and time stamped for logging purposes.

(14) There should be controls to verify that proper data is used when computerized data is entered into the computer application.

(15) When computerized files are entered into the computer application, there should be controls to verify that the proper version of the file is used.

(16) Application programs should include routines for checking internal file header labels before processing.

(17) Internal trailer labels should contain control totals to provide a check that all records are on the file.

(18) File completion checks should be performed to ensure that application files have been completely processed, including both transaction and master files.

(19) Record and predetermined control totals generated by the application should be used by the data processing control group to validate the completeness of data processed by the system.

(20) A direct update to files should cause creation of a record added to a backup file and recording of the transaction on the transaction history file.

(21) A "before and after picture" of the master file being updated should be maintained.

(22) Relationship editing should be performed between the input transaction and master files to check for appropriateness and corrections prior to updating.

(23) The data processing control group should balance batch counts, record counts, and predetermined control totals of data submitted for processing; ensure that input and/or work and/or output files used in computer processing are correct and maintained in logs; and ensure that restarts are properly performed.

g. Malfunction Reporting and Preventive Maintenance Controls

(1) The computer system should automatically produce a log of all-system operations.

(2) Disposition notes should be entered on the console log showing corrective actions taken when unscheduled program halts occur.

(3) Job reruns should be recorded along with their reason on the console log.

(4) The console log should include the date, job name and number, program name and number, start and/or stop times, files used, record counts, and scheduled and unscheduled halts.

(5) All computer time should be accounted for.

(6) Sensitive data should be removed from on-line storage devices before equipment is turned over to maintenance personnel.

(7) System reliability reports should include Mean Time Between Failures (MTBF) and Mean Time To Recovery (MTTR) statistics.

h. Data Output Controls

(1) The data processing organization should have a control group that is responsible for reviewing all outputs produced by the application.

(2) This group should reconcile each output batch total, record count and predetermined control total with input batch totals, and record counts and predetermined control totals before releasing any reports in order to ensure that no data was added or lost during processing.

(3) A transaction log kept by the application should be compared regularly with a transmission log kept at each output device to ensure that all transactions have been properly processed to the final output steps.

(4) The user should have a control group that is responsible for reviewing all output received from the data processing organization.

(5) System output logs should be kept to provide an audit trail for the outputs and to summarize the number of reports generated, the number of copies of each report, the recipients of each report and the report security status.

(6) Transactions should be able to be traced forward to the final outputs and backward to the original source documents.

(7) The cover sheet of every report should clearly identify the recipients' names and locations.

i. Data Communications Controls

(1) Controls over data communication devices should be established and followed to ensure accuracy and privacy of transmitted data. The following control techniques should exist within data communication devices:

(a) A unique hard-wired identification code, requiring no human intervention for its use, should be incorporated into each terminal device;

(b) The identification code should be checked and validated by the computer to ensure that no unauthorized terminals are being used;

(c) Conditioned lines should be used to reduce data transmission errors and to maintain integrity of data transmitted;

(d) Scrambling or encryption techniques should be used in transmitting classified data;

(e) An automatic store-and-forward capability should be used to maintain control over messages queued for an inoperative or for a busy communications device;

(f) Parity checks should be used to detect errors in the transmission of data;

(g) Validity checks should be used to compare characters so that erroneous data can be detected;

(h) Forward error correcting techniques should be used for the detection and reporting of data communications errors using sophisticated redundancy codes;

(i) Techniques should be available for detecting erroneous retransmissions of data;

(j) Modems should be equipped with loop-back switches for fault isolation.

(k) A message intercept function should be used to receive messages directed to inoperable or unauthorized terminals.

5. • Update Plans for Training, Log, Support, T&E, Development and Acquisition.

a. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

b. Workload Scheduling Controls

(1) A formal control group should be established within the data center to monitor both remote decentralized as well as centralized job entry.

(2) The control group should be responsible for recording and controlling the production data processed by the data processing organization.

(3) All totals should be balanced during and after applications processing, and all processing errors should be controlled by the control group.

(4) An authorization document or a transmittal sheet should be required to accompany all input transactions.

(5) All output reports should be visually scanned by the control group for general accuracy and completeness and be distributed according to a formal schedule.

(6) A priority scheme of classes or priorities should be used for scheduling work.

(7) Source documents should be maintained for reference in a logical sequence for a suitable period of time.

(8) A systematic time-related flow of jobs through each work center should be established.

c. Organizational Controls

(1) Transactions generally should originate and be authorized in an organization outside of ADP.

(2) Training programs should exist to maintain and build skills, knowledge and ability in systems technology, as well as internal control and ADP security requirements.

d. Internal Audit

(1) During system planning and development, internal audit should ensure that the system carries out prescribed management policies.

(2) Internal audit should review general controls in data processing systems to determine that controls have been designed according to management direction and legal requirements and that these controls are operating effectively to provide reliability of, and security over, the data being processed.

e. Distributed Processing and Network Operations Controls

(1) Each network message and/or transmitted data unit should contain codes that identify the sender and intended receiver(s).

(2) Adequate security should exist and be periodically reviewed over data controlled by network data base management systems and application and/or transaction processor, and over data handled at network processing facilities and remote locations.

(3) Review procedures for identifying and handling sensitive data should exist, and security classification for all levels of data sets in the network should be developed, consistent with information classification requirements.

(4) Procedures stating the preferred method for disposing of sensitive network documents at remote locations should exist and be communicated to the appropriate personnel.

(5) All outgoing messages and/or data units should be edited for valid destination addresses.

f. Disaster Avoidance and Recovery

(1) Procedures should include steps to be taken in the event of an actual or likely natural disaster by fire, water damage, and intentional damage by sabotage, mob action, bomb threats.

(2) Procedures should exist and be applied for the retaining and/or copying of master files as a means of reconstructing a damaged or destroyed file.

g. Data Communications Systems Controls

(1) A data communications system should serve as the interface between terminals and the central data processing system.

(2) The data communications system should control access to and use of terminals, poll and receive messages from computer terminals or other computers, address and send messages back to computer terminals or other computers, edit and format input and output messages, handle error situations, reroute traffic when terminals or lines are inoperative, and perform on-line formatting on visual display terminals.

6. • **Risk Analysis Reassessed.**

7. • **Economic Analysis Prepared (DoD Instruction 7041.3) (reference (q)).**

a. Distributed Processing and Network Operations Controls

(1) The decision to undertake distributed processing should be documented and supported by cost and/or benefit analysis studies.

(2) A cost and/or benefit analysis of encryption and private line acquisition should be made.

b. Systems Development Methodology Controls

(1) The system development process should include cost and/or benefit analysis.

(2) A cost and/or benefit analysis should be performed to ensure that the conceptual system will produce desired results economically.

(3) Additional hardware and system software requirements should be consistent with ADP plans and be included in the cost and/or benefit analysis, and be used to prepare the computer programs.

(4) The detailed system design should be consistent with the conceptual design, be based on the feasibility study and on the cost and/or benefit analysis, and be used to prepare the computer programs.

8. • **Configuration Management Discipline for Total AIS Developed.**

9. • **Computer Resource Acquisition Plans Finalized.**

a. AIS Planning

(1) The planing process should measure and compare actual accomplishments with expected performance throughout the system life cycle.

10. • **Preparation of System Decision Paper (SDP-II).**

a. Systems Development Methodology Controls

(1) The system development process should include detailed system analysis and design.

(2) The detailed system design should be consistent with the conceptual design, be based on the feasibility study and on the cost and/or benefit analysis, and be used to prepare the computer programs.

11. • **Submit SDP to LCM review and milestone approval authority.**

a. Policies, Standards, and Procedures

(1) Rigorous AIS budgeting procedures should be implemented to ensure that all significantly ADP-related initiatives, expenditures, and reprogramming are clearly highlighted, whether or not they fall within budget decision units or are spread over multiple decision units.

D. Development (Phase 3)

1. • **Mission Need Reaffirmed.**

a. AIS Planning

(1) Regular internal audit review and reporting should be conducted regarding completed and proposed planning decisions in relation to mission requirements.

2. • **Develop Computer Programs and Data Bases.**

a. AIS Planning

(1) The planning process should measure and compare actual accomplishments with expected performance throughout the system life cycle.

b. Systems Development Methodology Controls

(1) The system development process should include programming.

(2) Additional hardware and system software requirements should be consistent with AIS plans and be included in the cost and/or benefit analysis, and be used to prepare the computer programs.

(3) The detailed system design should be consistent with the conceptual design, be based on the feasibility study and on the cost-benefit analysis, and be used to prepare the computer programs.

(4) Program and system test results should be reviewed and signed by the system analyst.

(5) Sufficient computer time should be allocated for the conversion process.

(6) The system should be "acceptance tested" by a group independent of the programmers and analysts who designed the system to ensure that it performs in accordance with specifications and meets user needs.

(7) The system acceptance group should certify in writing that the system performs in accordance with all functional and performance specifications.

(8) This group should control all changes to the system to maintain its integrity on a continuing basis.

(9) The following personnel should be involved in the system development process: project managers users, system analysts, programmers, acceptance testers, and internal auditors.

(10) The duties of the personnel on the development project should be clearly separated.

(11) Specific tasks and timeframes for completing the tasks should be established for each member of the development project.

(12) The project manager should be authorized to make decisions on personnel resources, scheduling and most technical project matters.

(13) A management project steering committee should be formed to oversee and review progress throughout the life cycle.

(14) Users should actively participate in system development.

c. Program Testing and System Acceptance Controls

(1) Programming and software packages should be used to improve computer programs' efficiency and effectiveness.

3. • **System Support Documentation Developed (User's Manuals).**

a. Malfunction Reporting and Preventive Maintenance Controls

(1) Formal malfunction reporting procedures should be established and documented for the data processing installation.

(2) Computer operators should be required to keep logs of all computer processing actions.

(3) These logs should record start ups, errors, reruns, recoveries, shut downs, shift changes, and maintenance occurrences.

(4) Log pages should be sequentially numbered.

(5) All processes and operator decisions should be recorded chronologically in the operations log.

(6) Console log pages should be sequentially numbered.

(7) Formal preventive maintenance procedures should be established and documented for the data processing organization.

b. Technical Controls

(1) The vendor or developer of the security software should provide a completely documented description of its design and operation.

(2) Security software functions should be adequately supported by proper manual procedures.

(3) Library procedures should be documented.

(4) External labeling procedures should be documented.

c. Disaster Avoidance and Recovery

(1) These control procedures need to be formally documented and periodically tested and updated.

(2) Emergency procedures should be formally documented and distributed to all associated personnel.

(3) Backup arrangements should be documented and formally agreed upon by all parties concerned.

d. Operating Systems Controls

(1) A complete documented description of the operating system's design and operation should be provided by the vendor or developer.

e. System Utilities Controls

(1) The vendor or developer of the system utilities should provide a complete documented description of their design and operation.

(2) A complete directory of all available utilities should exist.

f. Program Library Systems Controls

(1) A program library system should be used to control application programs.

(2) The program library system should restrict access to application programs, control movement of programs from test to production modes, control movement of programs from source code to object code, and control changes to application programs.

(3) Control functions performed by the program library system should be protected so they cannot be bypassed.

(4) The vendor or developer of the program library system should provide a complete documented description of the system's design and operation.

(5) Program library system functions should be adequately supported by proper manual procedures.

g. File Maintenance Systems Controls

(1) The vendor or developer of the file maintenance system should provide a complete documented description of its design and operation.

(2) File maintenance system functions should be adequately supported by proper manual procedures.

h. Data Communications Systems Controls

(1) The vendor or developer of the data communications system should provide a complete documented description of its design and operation.

(2) Data communications system functions should be adequately supported by proper manual procedures.

i. System Software Change Controls

(1) All relevant documentation should be changed to reflect system software modifications.

(2) System software changes should be thoroughly tested to ensure that modifications function properly.

(3) System software modifications should be subjected to a system acceptance test before being placed in operations.

j. Distributed Processing and Network Operations Controls

(1) Summary control reports should be distributed to all network user organizations.

(2) Written procedures should exist for switching to backup equipment, files, or systems.

(3) Remote users should have a list of standard terminal, modem, and controller device settings to facilitate problem determination.

k. Systems Development Methodology Controls

(1) The system development process should include procedure preparation.

(2) Procedures should exist to ensure that no data is lost or erroneously changed during conversion to the newly designed system.

l. System Reporting Documentation Controls

(1) A plan should be documented to test the system.

(2) A test analysis report should be developed to document the test analysis results and findings.

(3) A users or procedures manual should be developed to document the functions of the system

(4) An operations manual should be developed to describe the system and its operational environment for computer operations personnel.

(5) A program maintenance manual should be developed to give the maintenance programmer sufficient information to understand the programs, their operating environment and their maintenance procedures.

(6) There should be signatures or other documented evidence of who performed systems and programming work.

(7) Ensure that programmers implement established standards for documenting different data processing functions.

m. Data Origination Controls

(1) Documented procedures should exist to explain the methods for source document error detection, correction, and reentry.

n. Data Input Controls

(1) Documented procedures should exist to explain the methods for data conversion and entry.

(2) Documented procedures should exist to explain the process of identifying, correcting, and reprocessing data rejected by the application.

o. Data Processing Controls

(1) Documented procedures should exist to explain the methods for proper data processing of each application program.

(2) Operator instructions should include system start-up procedures, backup assignments, emergency procedures, system shutdown procedures, error message debugging instructions, and system and job status reporting instructions.

p. Data Output Controls

(1) Documented procedures should exist to explain the methods for proper balancing and reconciliation of output products.

(2) Documented procedures should exist to explain the methods for proper handling and distribution of output reports.

q. Program Change Controls

(1) User authorization and written approval should be required for all program changes.

(2) AIS project management authorization and written approval should be required for all program changes.

4. • **Unit and System Level Test Performed.**

a. System Software Change Controls

(1) System software changes should be thoroughly tested to ensure that modifications function properly.

(2) System software modifications should be subjected to a system acceptance test before being placed in operations.

b. Distributed Processing and Network Operations Controls

(1) Users should participate in acceptance test, review test results, and provide approvals for functions over which they have jurisdiction.

c. Systems Development Methodology Controls

(1) The system development process should include testing.

(2) Upon completion of all programming, each program, interrelated subsystem and the entire system should be thoroughly tested.

(3) Program and system test results should be reviewed and signed by the system analyst.

(4) Prior to acceptance testing, the newly designed system should be tested in parallel operations with the old system.

d. System Reporting Documentation Controls

(1) A plan should be documented to test the system.

(2) A test analysis report should be developed to document the test analysis results and findings.

e. Program Testing and System Acceptance Controls

(1) Each program, subsystem, and then the entire system should be tested.

(2) Test data should be treated like live data, as opposed to entering codes in the test data to indicate that it is not normal production data. When using test data in a live system, it would be mandatory to make it as test data.

(3) System acceptance transactions should be tested like live transactions, as opposed to having special codes entered in the transaction to indicate that it is not normal production data.

(4) Sufficient volumes of test and system acceptance transactions that have a wide range of valid and invalid conditions should be entered and processed.

(5) Sufficient time should be allocated for thorough testing and system acceptance purposes.

(6) Sufficient staff members should be allocated for testing and system acceptance purposes.

(7) Test cases and system acceptance test transactions should be developed to review:

(a) Mainline and end-of-job logic.

(b) Each routine.

(c) Each exception.

(d) Abnormal end-of-job conditions.

(e) Combinations of parameter cards and switch settings.

(f) Unusual mixtures and sequences of data.

(g) Control features; e.g., salary parameters.

(8) Test and system acceptance data should include cases that test for the following:

(a) Codes.

(b) Characters.

(c) Fields

(d) Combination of fields.

(e) Transactions.

(f) Calculations.

(g) Missing data.

(h) Extraneous data.

(i) Amounts.

(j) Units.

(k) Composition.

(l) Logic decisions.

(m) Limit or reasonable checks.

(n) Sign.

(o) Record matches.

(p) Record mismatches.

(q) Sequence.

(r) Check digit.

(s) Crossfooting of quantitative data.

(t) Control totals.

(9) New programs should be run parallel to old ones to help ensure their accuracy.

5. • **Computer Resource Acquisition Strategy Implemented (hardware, software & services acquired).**

o Product Control Through Configuration Management Implemented.

a. Systems Development Methodology Controls

(1) The system development process should include operations.

6. • **Logistics Support and Training Plans Finalized.**

a. Organizational Controls

(1) Training programs should exist to maintain and build skills, knowledge and ability in systems technology, as well as internal control and ADP security requirements.

b. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

c. Distributed Processing and Network Operations Controls

(1) Documentation and training should be provided to all network operations personnel.

7. • Product Acceptance Criteria Finalized. Products Evaluated.

a. Internal Audit

(1) Internal audit should review application controls of computer-based systems to assess their reliability in processing data in a timely, accurate, and complete manner.

(2) These control reviews should ascertain whether the systems conform to both organization and Federal standards.

b. Systems Development Methodology Controls

(1) The system development process should include system acceptance.

(2) Upon completion of all programming, each program, interrelated subsystem, and the entire system should be thoroughly tested.

(3) The system should be "acceptance tested" by a group, independent of the programmers and analysts who designed the system, to ensure that it performs in accordance with specifications and meets user needs.

(4) The system acceptance group should certify in writing that the system performs in accordance with all functional and performance specifications.

c. Program Testing and System Acceptance Controls

(1) All computer programs should be checked by the programmer and his/her supervisor through desks checks or walk throughs before program assembly or compilation.

(2) All computer programs should be reviewed after assembly or compilation to ensure that errors disclosed by these routines are corrected.

(3) System acceptance should be performed using test data similar to, but independent of, program testing data.

(4) All computer-based systems should be subjected to a system-acceptance process.

(5) The system acceptance should evaluate whether the entire system, both manual and automated processes, is performing in accordance with system specifications and processing standards.

(6) System acceptance should be performed by individuals independent of those who performed the analysis, design, and/or development of the system.

(7) Once system acceptance has been completed, a written certification that the entire system performs in accordance with all functional and performance specifications should be required before the system is placed in operation.

8. • **Operations and Deployment Plans Finalized.**

a. Organizational Controls

(1) The ADP function should be placed sufficiently high in the organization to ensure its independence from other site operations.

(2) Major organizational units within ADP should be described and their responsibilities delineated and documented.

(3) Where practical, the following functions should be performed by a different individual or group:

(a) Systems analysis.

(b) Application programming.

(c) Acceptance testing.

(d) Program change control.

(e) Data control.

(f) Production control and scheduling.

(g) Computer equipment operation.

(h) System software maintenance.

(i) Computer files maintenance.

(j) Source document origination.

(k) Source document conversion to machine-readable format.

(4) Transactions generally should originate and be authorized in an organization outside of ADP.

b. User Billing and Charge-back Controls

(1) Procedures for user billing and charge should be documented.

(2) Billing and charge-back agreements should exist between users and the data processing organization.

(3) The user billing charge-back procedures should be effectively tied into a job accounting system for the data processing resources.

(4) The user billing and charge-back procedures should be based on the number of transactions processed, on an artificial "computer accounting unit", or some other equitable method.

(5) Adequate procedures should exist for determining the share of system development costs plus additional overhead items, such as lighting, space, and air conditioning, for billing users.

(6) Additions and replacements of hardware, software, should be justified on the basis of resource utilization and user needs.

(7) An equitable procedure should exist for charging reruns of productions jobs so that user errors are charged back to users, while data processing organization errors are absorbed by data processing.

c. Workload Scheduling Controls

(1) The control group should establish and document formal scheduling procedures, schedule production runs and other workloads, and reschedule aborted or erroneous processing.

(2) The control group should be responsible for recording and controlling the production data processed by the data processing organization.

d. System Software Change Controls

(1) Formal documented system software change procedures should be established.

(2) Procedures should be established to ensure that emergency system software modifications are immediately subjected to a system acceptance test.

(3) Procedures should be established so that the accepted emergency modifications will be incorporated into the next operational version of the system software.

e. Distributed Processing and Network Operations Controls

(1) The distributed processing requirements definitions should be responsive to management objectives in

terms of the hardware configuration, data base configuration, and hardware and communications network interface.

(2) Network data policies should require that data set ownership be clearly established.

(3) User and system responsibilities should be fully defined for coordinating and reconciling differences between distributed and/or replicated data bases prior to network implementation.

(4) Reconciliations should be able to be satisfactorily performed under normal conditions, following network failures, and between varying application problems.

(5) Network asset inventories should be maintained at respective facilities and be periodically reviewed against actual network facilities.

(6) Effective hardware and software backup provisions should exist for the entire network and for the individual facility.

(7) Local and consolidated network performance reports should be established to regularly report key elements such as network system availability, performance to schedules, response times, processing facility efficiencies and performance problems.

f. Data Origination Controls

g. Data Input Controls

9. • **Economic Analysis Updated**

a. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

10. • **Preparation of System Decision Paper (SDP III).**

11. • **Submit SDP to LCM review and milestone approval authority.**

a. Policies, Standards, and Procedures

(1) Rigorous ADP budgeting procedures should be implemented to ensure that all significantly AIS-related initiatives, expenditures, and reprogramming are clearly highlighted, whether or not they fall within budget decision units or are spread over multiple decision units.

E. Deployment (Phase 4) and Operation (Phase 5)

1. • Implement Operational And Deployment Schedule

a. Administrative Controls

(1) Risk assessment studies should be performed at least every 5 years.

(2) The mission analysis process should be considered an on-going, continuous process through the life cycle, to ensure that both present and future data processing needs are satisfied.

(3) Requirements should be established for conducting risk analysis for DoD Government-owned, contractor-operated facilities and for Government-operated facilities.

(4) Responsibility should be assigned for computer security at each ADP facility.

(5) Individuals assigned responsibility for computer security should be given training and experience in both the computer and security areas.

(6) Plans should provide for assessing risks related to computer services provided by other agencies and those provided through commercial services.

(7) Employees utilizing ADP equipment and processing DoD data should be required to sign an agreement regarding their role and responsibility at the facility and in the ownership and use of data processing equipment and information within the data center.

(8) Personnel security policies for screening employees and contractor and/or service personnel should be established and provide for levels of screening comMNSurate with the sensitivity of the position or function.

(9) Procedures should exist to handle a situation in which an employee becomes a suspected security risk.

b. Physical Controls

(1) Written procedures should exist to define restrictions to computer room access.

(2) A reliable guard service or alarm system should exist to protect the computer center against illegal entry, vandalism, or sabotage.

(3) Access to the computer areas should be restricted to only authorized and appropriate personnel through

the use of a passcard system, combination locks, security badges, or other appropriately secure means.

(4) Combinations on locks or similar devices should periodically be changed.

(5) Account codes, authorization codes, passwords, should be controlled to prevent unauthorized use.

(6) Restricted entrances and emergency exits should be equipped with tamperproof automatic alarm systems that signal when doors are opened.

(7) Exterior walls, tape library walls, storage room walls, should be of solid construction from floor to ceiling.

(8) Data processing personnel should be trained to challenge improperly identified visitors.

(9) Data processing personnel should be counseled to report all intentional or inadvertent cases of security intrusions of which they become aware.

(10) Access to the computer area by custodial, electrical and other in-house maintenance personnel should be supervised and controlled.

(11) Vendor and support personnel should provide positive identification before they can be admitted to the computer area.

(12) At least two individuals should be present in the computer room at all times.

(13) A procedure should exist to restrict access to source documents and blank input forms to authorized employees.

(14) All critical forms, such as identification cards, negotiable instruments, and source documents, should be prenumbered for accountability, stored in a secure location, and periodically accounted for.

(15) Procedures should exist to limit access to critical forms during their intermediate storage and transportation, such as dual custody and mail message carrier controls.

(16) A procedure should exist for joint authorization of releases from the storage areas, and the receipt of critical forms should be inventoried by two people at the time of delivery.

(17) Procedures should be established to control the issuance of critical forms for jobs scheduled for processing.

(18) Copies of critical outputs that need to be destroyed should be kept in a secure location until they can be destroyed.

(19) At least two people should be present when critical outputs are destroyed.

(20) Periodic billing statements should be provided to user departments describing cost details and the billing algorithm used.

c. Disaster Avoidance and Recovery

(1) The computer center should be separated from adjacent areas by fire resistant partitions and/or walls, and non combustible materials should be used in the center.

(2) Emergency procedures for handling minor and major fires should be prominently posted throughout the data center.

(3) Heat and smoke detectors should be installed in the ceiling, under raised floors, and in the air ducts, alerting the local fire department as well as internal personnel.

(4) Portable fire extinguishers should be located in strategic and accessible areas, be vividly marked, and be periodically tested.

(5) Emergency exits and evacuation routes should be clearly labeled, and battery-powered emergency lights should be placed in strategic locations to assist in evacuation should the power be interrupted.

(6) The computer center should be protected by an automatic fire suppression system.

(7) Emergency switches for cutting off power should be easily accessible near the data center exits.

(8) Emergency power shutdown should include the air conditioning system.

(9) Either the computer center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and humidity in the computer center and take appropriate actions as necessary.

(10) The computer center should be air conditioned by a separate system sufficiently protected from unauthorized access and made from noncombustible materials.

(11) Air intakes should be protected against the introduction of noxious substances.

(12) Backup air conditioning should be available.

(13) The source of electric power should be sufficiently reliable to ensure continued operations and be adequately protected from unauthorized access.

(14) The computer center should be backed up by an uninterruptible power source system.

(15) At least one file generation should be kept at a location other than the file storage area.

(16) Copies of critical files, application programs, system software programs and critical documentation should be stored at an off-site location and be restricted from unauthorized access.

(17) Backup computer capacity should exist within the computer center and at an off-site location.

(18) Critical locations should be provided with the backup devices of terminals, modems, and communication lines.

d. Technical Controls

(1) A list of all personnel should exist and be periodically reviewed by supervisors detailing what computer resources the personnel have access to.

(2) The responsibility for issuing and storing disk packs, magnetic tapes, or other data storage media should be assigned to a librarian. This responsibility should be the librarian's chief function.

(3) Library procedures should be documented.

(4) Access to the library should be limited to authorized personnel.

(5) A librarian should be on duty whenever the data center is being used.

(6) Sensitive files, such as security classifications or Privacy Act restrictions (reference (1)), should be properly identified as such, and appropriately secured.

(7) To prevent release to unauthorized personnel, all data files should be logged in and out.

(8) All files should be expeditiously returned to the library after use.

(9) Disk packs and tape inventory records should be kept.

(10) External labeling procedures should be documented.

(11) External labels should be affixed to active disks and/or tapes.

(12) Work or scratch tapes should be kept in separate areas of the library.

e. AIS Planning

(1) Regular internal audit review and reporting should be conducted regarding completed and proposed planning decisions in relation to mission requirements.

f. Policies, Standards, and Procedures

(1) All appropriate organizational components of the site involved with ADP systems should be defined and clearly assigned their respective areas of functional responsibility.

g. Distributed Processing and Network Operations Controls

(1) Documentation and training should be provided to all network operations personnel.

(2) Network asset inventories should be maintained at respective facilities and be periodically reviewed against actual network facilities.

(3) Effective hardware and software backup provisions should exist for the entire network and for the individual facility.

(4) Procedures stating the preferred method for disposing of sensitive network documents at remote locations should exist and be communicated to the appropriate personnel.

(5) Network availability and reporting, timing and/or response, storage, backup, and functional control requirements for all applications should be established by users and communicated to the responsible network operations organization.

(6) All network facilities should communicate with each other on a regular basis to discuss schedules and coordinate processing requirements and operating procedures.

(7) All network facilities should prepare schedules of consumable needs so that resources can be efficiently and effectively distributed throughout the network.

(8) Remote and local network control terminals, and operations personnel authorized to use them, should be identified.

(9) All outgoing messages and/or data units should be edited for valid destination addresses.

(10) When encryption is in use, the individual assigned the responsibility of management should not be involved with the operation or processing of data.

(11) Remote users should have a list of standard terminal, modem, and controller device settings to facilitate problem determination.

(12) Local and consolidated network performance reports should be established to regularly report key elements, such as network system availability, performance to schedules, response times, processing facility efficiencies and performance problems.

(13) External labels should be used on cables, modems, control units, and other hardware devices to expedite fault isolation and service.

(14) Communications provisions should exist to temporarily store messages and/or data units destined for remote facilities not in service and for reactivating them when service is resumed.

(15) Procedures should exist at remote facilities to ensure that all changes made to operating systems software are effectively controlled and made immediately visible to the control group directly responsible for the overall network.

(16) Local and/or private communications lines and switches should be adequately secured and accessible only by authorized personnel.

(17) Consolidated security reports should be periodically published reflecting recent network security reviews, and they should be available to all network user organizations.

(18) Adequate security measure should be in force at the backup facility.

h. Data Origination Controls

(1) This control group should verify that source documents are complete and accurate. Furthermore, all documents should be accounted for, be transmitted in a timely manner and have been appropriately authorized.

(2) A separate user group should perform the input function when the user organization is responsible for its own data entry.

(3) The control group should identify errors to facilitate the timely correction of erroneous information.

(4) Error logs should be used to ensure timely follow-up and correction of unresolved errors.

(5) Originators of source documents should be notified by the control group of all errors.

(6) Blank source documents should be stored in a secure location.

(7) When transmitted for conversion, source documents should be transported in accordance with their security classifications.

(8) Source documents should be retained as a safeguard against data loss or destruction during subsequent processing.

(9) Source documents should have specific retention periods.

(10) Source documents should be stored in a logical manner to facilitate retrieval.

(11) Whenever a source document leaves the originating organization, a copy should be kept in the organization.

(12) When reaching their expiration dates, source documents should be removed from storage and destroyed in accordance with the approved disposal schedule.

i. Data Input Controls

(1) Data entry terminal devices should be locked in a physically secure room.

(2) The work entered on a terminal should be restricted by the authority level assigned to each terminal.

(3) Individual passwords should be changed periodically.

(4) Passwords should be deleted once an individual changes his or her job function or level of access.

(5) Management should review unauthorized usage reports.

(6) Management should periodically review the propriety of the terminal authority levels.

(7) Each individual user of the on-line system should be limited to certain types of transactions.

(8) Corrections should be reviewed and approved by supervisors before reentry, if appropriate.

(9) Procedures for processing corrected transactions should be the same as those for processing original transactions, except for the supervisory review and approval.

(10) The ultimate responsibility for the completeness and accuracy of all application processing should remain with the user.

(11) The terminal user should correct errors caused by data conversion or entry.

(12) The user originating the transaction should correct errors not caused by data conversion or entry.

(13) Debit and/or credit entries, rather than delete or erase commands, should be used to correct errors on the suspense file.

(14) All documents entered into the application should be signed or marked in some way to prevent accidental duplication or reuse of the data.

(15) The data processing organization should have a schedule by application showing when data requiring conversion and when data requiring entry will be received and needs to be completed.

(16) The data processing organization should have a control group responsible for data conversion and entry of all source documents received from users.

(17) This group should account for all batches of source documents received from the user to ensure that no batches have been added or lost.

(18) This group should independently develop record counts and predetermined control totals to be balanced with those of the control group in the user organization, and all discrepancies should be reconciled.

j. Data Processing Controls

(1) The data processing organization should have a schedule showing when each application program is to be run and needs to be completed.

(2) The data processing organization should have a control group responsible for controlling all data processing operations.

(3) The log should routinely be reviewed by supervisors to determine the cause of problems and the appropriateness of actions taken.

k. Data Output Controls

(1) The data processing organization should have a control group that is responsible for reviewing all outputs produced by the application.

(2) This group should monitor the processing flow to ensure that programs are processed according to schedule.

(3) This group should review output products for general acceptability and completeness.

(4) This group should reconcile each output batch total, record count and predetermined control total with input batch totals, record counts and predetermined control totals before releasing any reports to ensure that no data was added or lost during processing.

(5) These logs should be reviewed by supervisors to determine the correctness of output production.

(6) A transaction log kept by the application should be compared regularly with a transmission log kept at each output device to ensure that all transactions have been properly processed to the final output steps.

(7) The user should have a control group that is responsible for reviewing all output received from the data processing organization.

(8) This group should be given lists of all changes to the application master file data and programmed data, of all internally generated transactions produced by the application, of all interface transactions processed by the application, and of all transactions entered into the application.

(9) This group should use these lists to verify the accuracy and completeness of all output.

(10) This group should verify all computer-generated batch totals, record counts and predetermined control totals with its own manually developed batch totals, and record counts and predetermined control totals.

(11) The user should retain ultimate responsibility for the accuracy of all outputs.

(12) A priority system should exist to ensure that critical outputs are produced on time.

2. • **Formal Change Control Process.**

a. System Software Change Controls

(1) Formal documented system software change procedures should be established.

(2) Change request forms or other documentation should be used to originate system software modifications, with all forms sequentially numbered and accounted for.

(3) Access to data files and application programs should be denied to the system programmer making a system software modification.

(4) The system programmer making an emergency modification should be denied access to data files and application programs that were operating when the problem occurred.

(5) The system programmer making an emergency system software modification should complete a signed statement and leave it with the computer operator as to the encountered problem and its solution.

b. Systems Development Methodology Controls

(1) This group should control all changes to the system to maintain its integrity on a continuing basis.

(2) System implementation should be coordinated with all personnel involved and other systems affected.

c. Program Change Controls

(1) Formally approved written standards for program changes and documentation should exist and be followed.

(2) Procedures defining who can initiate and who can authorize change requests should be established.

(3) Change requests should be written, including a description of the nature of and reasons for the proposed change as well as security and privacy specifications.

(4) Change requests should be made by users on sequentially numbered forms.

(5) User authorization and written approval should be required for all program changes.

(6) AIS project management authorization and written approval should be required for all program changes.

(7) Changes should be approved by individuals who do not operate the computer, except for microcomputers.

(8) Procedures should exist to ensure that all program changes, both scheduled and emergency, are subjected to the testing and acceptance process.

(9) Application changes should be tested prior to operational use.

(10) Modified programs should be tested under normal operating conditions.

(11) Users should be involved in preparing test data and reviewing test results.

(12) Test results should be reviewed with supervisory personnel before revisions become effective.

(13) All errors detected during the conversion process should be investigated before and after correction.

(14) Certification should be made that test results demonstrate adequate protection from fraud, waste, and misuse of the program.

(15) All program changes should be documented, and appropriate program, system, operations, and user documentation should be updated as changes are made.

(16) A log should be maintained of all completed changes and all changes in progress.

(17) Program changes should be documented by individuals who do not operate the computer.

(18) Certification should be made that documentation specifications are met.

(19) Program library software should be used to report all changes to ADP managers and to users.

(20) Assurances should be made that changes meet users' needs.

(21) Procedures should exist to determine if any other system is affected by the program modification.

(22) Original programs should be retained until changes have been processed and new programs tested and updated.

(23) Once modifications have been implemented, procedures should prevent original programs from being used by mistake.

(24) Procedures should be in place to ensure that an "abnormal" volume of regularly scheduled program modifications results in a review to determine if a problem exists with programs, procedures, or the computer-based system.

(25) A limit should be placed on the frequency of program changes, except for emergency changes.

(26) When emergency changes are made, both the user and ADP project manager should be notified.

(27) All problems related to program changes should be documented and given to the ADP project manager.

3. • **Periodic Reviews and Audits.**

a. AIS Planning

(1) AIS planning should be related to budgeting for financial, personnel, and system resources.

(2) The planning process should measure and compare actual accomplishments with expected performance throughout the system life cycle.

b. Internal Audit

(1) The internal auditors charter should allow the conduct of independent reviews and the reporting of findings and recommendations to the site's management.

(2) Periodic audits should be designed to test both internal controls and reliability of processed data.

(3) When appropriate, internal audit should verify the information on output reports against related source documents.

c. Workload Scheduling Controls

(1) A formal control group should be established within the data center to monitor both remote decentralized as well as centralized job entry.

(2) Formal input and/or output control procedures should be established and documented.

(3) All totals should be balanced during and after applications processing, and all processing errors should be controlled by the control group.

(4) An authorization document or a transmittal sheet should be required to accompany all input transactions.

(5) All output reports should be visually scanned by the control group for general accuracy and completeness and be distributed according to a formal schedule.

(6) A priority scheme of classes or priorities should be used for scheduling work.

(7) Source documents should be maintained for reference in a logical sequence until the scheduled time of disposal.

(8) The mix of on-line and batch jobs should be scheduled to promote efficient use of facilities and to meet user requirements.

(9) A systematic time-related flow of jobs through each work center should be established.

(10) Rush or rerun jobs should be scheduled consistent with their priority ratings.

(11) Approximate elapsed time of delay should be recorded for each delay event.

(12) In on-line systems, response time statistics should be kept and monitored for significant fluctuations in response time.

(13) CPU utilization statistics should be monitored for both batch and on-line processing.

(14) Significant variances in performance should be followed up by the control group.

d. Malfunction Reporting and Preventive Maintenance Controls

(1) The computer system should automatically produce a log of all system operations.

(2) Disposition notes should be entered on the console log showing corrective actions taken when unscheduled program halts occur.

(3) Job reruns should be recorded along with their reason on the console log.

(4) Logs should be reviewed and signed at the end of each shift by a supervisor and filed according to the authorized retirement schedule.

(5) Logs should be independently examined to detect operator problem and unauthorized intervention.

(6) System crashes should be isolated and identified by cause.

(7) System performance records should be maintained.

(8) Logs of the type and time of maintenance performed should be kept.

(9) A schedule for machine maintenance should be published and followed.

(10) The production schedule should be flexible enough to accommodate preventive maintenance.

(11) Preventive maintenance should not be scheduled during peak load periods.

(12) Rush or rerun jobs should be scheduled consistent with their priority ratings.

(13) Approximate elapsed time of delay should be recorded for each delay event.

(14) In on-line systems, response time statistics should be kept and monitored for significant fluctuations in response time.

(15) CPU utilization statistics should be monitored for both batch and on-line processing.

e. User Billing and Charge-back Controls

(1) Billing and charge-back agreements should exist between users and the data processing organization.

(2) The user billing charge-back procedures should be effectively tied into a job accounting system for the data processing resources.

(3) The user billing and charge-back procedures should be based on the number of transactions processed, on an artificial "computer accounting unit," or some other equitable method.

(4) Adequate procedures should exist for determining the share of system development costs plus additional overhead items, such as lighting, space, and air conditioning, for billing users.

(5) Additions and replacements of hardware, software, should be justified on the basis of resource utilization and user needs.

(6) Periodic billing statements should be provided to user departments describing cost details and the billing algorithm used.

f. Disaster Avoidance and Recovery

(1) These control procedures need to be formally documented and periodically tested and updated.

g. Distributed Processing and Network Operations Controls

(1) All network locations should receive regularly scheduled hardware preventive maintenance and log all hardware problems.

(2) A comprehensive post-implementation technical review of the network should be required and performed by systems personnel.

h. Systems Development Methodology Controls

(1) The system development process should include post-implementation audit.

(2) A post-implementation audit of the entire system, manual and automated, should be performed by the internal audit staff after the system has been in operation for several months.

i. Data Input Controls

(1) The suspense file should periodically be analyzed to determine whether too many errors are being made and whether corrections are being processed in a timely manner.

(2) The data processing organization should have a schedule by application showing when data requiring conversion and when data requiring entry will be received and needs to be completed.

(3) The control group should account for all batches of source documents received from the user to ensure that no batches have been added or lost.

(4) This group should independently develop record counts and predetermined control totals to be balanced with those of the control group in the user organization, and all discrepancies should be reconciled.

j. Data Output Controls

(1) Users should periodically be questioned to determine whether they find the reports they receive relevant; whether they find the data presented on reports accurate, reliable and useful; whether they should be removed from or added to distribution lists for receiving reports; and whether they have suggestions concerning the format, content, frequency, and timeliness of reports they receive.

k. System Utilities Controls

(1) Computer operators should be denied access to system utility documentation.

l. Program Library Systems Controls

(1) Computer operators should be denied access to all libraries maintained by the program library system.

4. • Maintain AIS Supporting Documentation

a. File Maintenance Systems Controls

b. Disaster Avoidance and Recovery

(1) Backup procedures should be periodically tested.

(2) Data center personnel should be trained periodically in fire-fighting techniques and be assigned individual responsibilities in case of fire.

(3) Either the computer center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and humidity in the computer center and take appropriate actions as necessary.

(4) A priority scheme should be established at the site and be approved by management, in the event that backup arrangements must be used.

(5) Computer operators should be denied access to all libraries maintained by the program library system.

c. Distributed Processing and Network Operations Controls

(1) Written procedures should exist for switching to backup equipment, files or systems.

d. System Reporting Documentation Controls

(1) Program and system documentation should be accessible to computer operations personnel.

(2) All documentation should be periodically reviewed to ensure that it is current and complete and adheres to established standards.

(3) Copies of all documentation should be stored off the premises.

(4) There should be signatures or other documented evidence of who performed systems and programming work.

(5) Documented procedures should exist for controlling all system documentation.

e. General Environmental Controls

5. • **Management and ADP Personnel Concern in Internal Control Techniques.**

a. Policies, Standards and Procedures

(1) All appropriate organizational components of the site involved with ADP systems should be defined and clearly assigned their respective areas of functional responsibility.

(2) Customer and/or service interface personnel should be assigned.

(3) ADP resources acquisition, system design, programming, and operating standards should be established, coordinated and communicated to all affected personnel.

b. Organizational Controls

(1) All ADP employees should be prohibited from having authority or duties in any other organization, unless authorized by management.

(2) A direct line of responsibility should exist between every subordinate and supervisor.

(3) A personnel rotation plan should be in effect within the different functional areas in the ADP organization.

(4) ADP personnel should be encouraged to take regularly scheduled vacations.

(5) Absentee and turnover rates in the ADP organization should be monitored for potential personnel problems.

(6) ADP position descriptions should be in writing, be clear in delineating authority and responsibility, be kept current, be accompanied by definitions of technical skills needed, and be usable as a basis for performance evaluation.

(7) Personnel recruiting and promotion practices should be based on objective criteria and should consider education, experience, and security risks relevant to the job requirements and to the degree of responsibility.

(8) Before being hired, ADP personnel should be subjected to preemployment checks.

(9) When hired, employees should be provided with an orientation of internal controls and security and with ongoing training to maintain their technical knowledge, skills, and abilities.

(10) Employee performance should be evaluated on a regular basis, and any negative performance should be appropriately addressed.

(11) Policies should be established allowing only authorized personnel use of microcomputer resources to protect the data, software, and physical equipment from improper use or theft.

(12) Proprietary software packages should be protected against copying or modification.

(13) A formal document should state that copyright laws will be rigidly enforced.

(14) Codes, passwords, or other devices should be used to identify authorized users of the microcomputers.

(15) When they are away from the microcomputer area, users of sensitive data should securely lock up all diskettes.

(16) Rooms in which microcomputers are located should be locked after normal working hours.

(17) Microcomputers should be stored in a controlled area.

(18) Property management procedures concerning microcomputer components should be followed, including marking them with unique identification numbers, and recording and securely storing all identification numbers, serial numbers, and equipment descriptions.

c. Workload Scheduling Controls

(1) All personnel should have a copy of a manual detailing required control procedures.

(2) Users should be involved with workload scheduling, except in emergencies.

(3) Operators should not be involved with workload scheduling, except in emergencies.

(4) Reasons for schedule delays should be identified by area of responsibility.

(5) Significant variances in performance should be followed up by the control group.

d. Malfunction Reporting and Preventive Maintenance Controls

(1) Operators and all other appropriate personnel should have access to a manual detailing these control procedures and certify in writing that they have reviewed and understood them.

e. User Billing and Charge-back Controls

(1) Billing and charge-back agreements should exist between users and the data processing organization.

(2) Additions and replacements of hardware, software, should be justified on the basis of resource utilization and user needs.

(3) Rates charged to users should encourage the use of data center resources in accordance with users' needs; differential rates for off-peak usage or the assignment of processing priorities for varying turnaround requirements should

be used to encourage maximum usage of centralized computer facilities.

f. Administrative Controls

(1) Responsibility for conducting risk analyses should be formally assigned.

(2) Responsibility should be assigned for computer security at each ADP facility.

(3) Individuals assigned responsibility for computer security should be given training and experience in both the computer and security areas.

(4) Employees utilizing ADP equipment and processing DoD data should be required to sign an agreement regarding their role and responsibility at the facility and in the ownership and use of data processing equipment and information within the data center.

(5) Personnel security policies for screening employees and contractor and/or service personnel should be established and provide for levels of screening commensurate with the sensitivity of the position or function.

(6) When an employee is terminated, the employee should immediately be denied access to the data processing organization, any data, program listings, and all other employees should be informed of the employee's termination.

g. Disaster Avoidance and Recovery

(1) Emergency procedures should be formally documented and distributed to all associated personnel.

(2) Procedures should include steps to be taken in the event of an actual or likely natural disaster by fire, water damage, and intentional damage by sabotage, mob action, bomb threats.

(3) The computer center should be separated from adjacent areas by fire resistant partitions and/or walls, and noncombustible materials should be used in the center.

(4) Smoking should be prohibited in the data center.

(5) Data center personnel should be trained periodically in fire-fighting techniques and be assigned individual responsibilities in case of fire.

(6) Emergency procedures for handling minor and major fires should be prominently posted throughout the data center.

(7) Heat and smoke detectors should be installed in the ceiling, under raised floors, and in the air ducts, alerting the local fire department as well as internal personnel.

(8) Portable fire extinguishers should be located in strategic and accessible area, be vividly marked, and be periodically tested.

(9) Emergency exits and evacuation routes should be clearly labeled, and battery-powered emergency lights should be placed in strategic locations to assist in evacuation should the power be interrupted.

(10) The computer center should be protected by an automatic fire suppression system.

(11) Emergency switches for cutting off power should be easily accessible near the data center exits.

(12) Emergency power shutdown should include the air conditioning system.

(13) Either the computer center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and humidity in the computer center and take appropriate actions as necessary.

(14) The computer center should be air conditioned by a separate system sufficiently protected from unauthorized access and made from noncombustible materials;

(15) Air intakes should be protected against the introduction of noxious substances.

(16) Backup air conditioning should be available.

(17) The source of electric power should be sufficiently reliable to ensure continued operations and be adequately protected from unauthorized access.

(14) The computer center should be backed up by an uninterruptible power source system.

(15) Procedures should exist and be applied for the retaining and/or copying of master files as a means of reconstructing a damaged or destroyed file.

(16) Sufficient generations of files should be maintained to facilitate reconstruction of records.

(17) At least one file generation should be kept at a location other than the file storage area.

(18) Copies of critical files, application programs, system software programs, and critical documentation should be stored at an off-site location and be restricted from unauthorized access.

(19) Backup computer capacity should exist within the computer center and at an off-site location.

(20) Critical locations should be provided with the backup devices of terminals, modems, and communication lines.

(21) Backup arrangements should be documented and formally agreed upon by all parties concerned.

(22) A priority scheme should be established at the site and be approved by management in the event that backup arrangements must be used.

(23) Backup procedures should be periodically tested.

(24) Off site materials should be periodically tested.

h. Physical Controls

(1) Data processing personnel should be trained to challenge improperly identified visitors.

(2) Data processing personnel should be counseled to report all intentional or inadvertent cases of security intrusions of which they become aware.

(3) Access to the computer area by custodial, electrical, and other in-house maintenance personnel should be supervised and controlled.

(4) Vendor and support personnel should provide positive identification before they can be admitted to the computer area.

i. Technical Controls

(1) The responsibility for issuing and storing disk packs, magnetic tapes, or other data storage media should be assigned to a librarian.

(2) The responsibility referenced in item 11, above, should be the librarian's chief function.

(3) A librarian should be on duty whenever the data center is being used.

j. System Utilities Controls

(1) Computer operators should be denied access to system utility documentation.

(2) Management authorization should be required prior to the installation and use of new releases of utility programs.

k. Program Library Systems Controls

(1) Obsolete programs should regularly be deleted from the source code and object code library.

l. Data Communications Systems Controls

(1) The authorization code should identify the individual using the terminal and should be periodically changed.

m. System Software Change Controls

(1) Computer operations personnel should have a list of system programmers to notify if the system software requires an emergency or immediate modification.

(2) Access to data files and application programs should be denied to the system programmer making a system software modification.

(3) The system programmer making an emergency modification should be denied access to data files and application programs that were operating when the problem occurred.

(4) The system programmer making an emergency system software modification should complete a signed statement and leave it with the computer operator as to the encountered problem and its solution.

n. Distributed Processing and Network Operations Controls

(1) Effective hardware and software backup provisions should exist for the entire network and for the individual facility.

(2) Adequate disaster and recovery procedures should be developed for each network processing facility. These procedures should be current and periodically tested.

(2) All network facilities should prepare schedules of consumable needs so that resources can be efficiently and effectively distributed throughout the network.

(4) Records should be maintained on the amount of resources used by each facility.

(5) A comprehensive post-implementation technical review of the network should be required and performed by systems personnel.

(6) A central control function should be established to coordinate control reviews of network assets and resources at all network locations.

(7) Control reviews should be used for assessing the ongoing integrity and overall control of the physical network.

(8) Network output requirements, operating schedules, processing procedures, and facility coordination policies should be fully established.

(9) Policy agreements should exist for communications transmissions including provisions to effectively interface software applications and data bases among coordinated network facilities.

(10) The assignment of transmission priorities should be consistent with established policy and appropriate for the need of the on-line application.

(11) Proper access control should be maintained over the storage and use of network test equipment.

(12) Adequate controls and training regarding distributed data should exist to ensure data compatibility, integrity and effective data usage.

(13) Documentation and training should be provided to all network operations personnel.

i. Systems Development Methodology Controls

(1) The systems acceptance group should control all changes to the system to maintain its integrity on a continuing basis.

6. • Risk Analysis Reassessed.

a. Disaster Avoidance and Recovery

(1) Emergency procedures should be formally documented and distributed to all associated personnel.

(2) The computer center should be separated from adjacent areas by fire resistant partitions and/or walls, and noncombustible materials should be used in the center.

(3) Smoking should be prohibited in the data center.

(4) Data center personnel should be trained periodically in fire-fighting techniques and be assigned individual responsibilities in case of fire.

(5) Emergency procedures for handling minor and major fires should be prominently posted throughout the data center.

(6) Heat and smoke detectors should be installed in the ceiling, under raised floors and in the air ducts, alerting the local fire department as well as internal personnel.

(7) Portable fire extinguishers should be located in strategic and accessible area, be vividly marked, and be periodically tested.

(8) Emergency exits and evacuation routes should be clearly labeled, and battery-powered emergency lights should be placed in strategic locations to assist in evacuation should the power be interrupted.

(9) The data center should be protected by an automatic fire suppression system.

(10) Emergency switches for cutting off power should be easily accessible near the data center exits.

(11) Emergency power shutdown should include the air conditioning system.

(12) Emergency procedures for handling minor and major fires should be prominently posted throughout the data center.

(13) The computer center should be air conditioned by a separate system sufficiently protected from unauthorized access and made from noncombustible materials.

(14) Either the data center should be equipped with temperature and humidity gauges that automatically activate warning signals if either moves outside the normal range, or personnel on duty should periodically check the temperature and

humidity in the computer center and take appropriate actions as necessary.

(15) The data center should be air conditioned by a separate system sufficiently protected from unauthorized access and made from noncombustible materials.

(16) Air intakes should be protected against the introduction of noxious substances.

(17) Backup air conditioning should be available.

(18) The source of electric power should be sufficiently reliable to assure continued operations and be adequately protected from unauthorized access.

(19) The computer center should be backed up by an uninterruptible power source system.

(20) Sufficient generations of files should be maintained to facilitate reconstruction of records.

(21) At least one file generation should be kept at a location other than the file storage area.

(22) Copies of critical files, application programs, system software programs and critical documentation should be stored at an off-site location and be restricted from unauthorized access.

(23) Backup computer capacity should exist within the data center and at an off-site location.

(24) Critical locations should be provided with the backup devices of terminals, modems, and communication lines.

(25) Backup arrangements should be documented and formally agreed upon by all parties concerned.

o (26) A priority scheme should be established at the site and be approved by management, in the event that backup arrangements must be used.

(27) Backup procedures should be periodically tested.

(28) Off-site materials should be kept up-to-date.

b. Microcomputer Controls

(1) User groups should be required to provide program documentation for approval prior to using application software developed by the group.

(2) A procedures manual should be developed to document the functions and capabilities of microcomputer-based systems.

(3) Approval, requisition, and subsequent placement of microcomputers should be documented.

(4) Management approval and user group concurrence should be secured in instances when data processing personnel modify application software packages.

(5) Management approval should be secured before application software packages are modified by user groups.

(6) Procedures related to sharing application programs and data should be established.

(7) Management should be established allowing only authorized personnel use of microcomputer resources to protect the data, software, and physical equipment from improper use or theft.

(8) Personnel with appropriate backgrounds should be designated to develop application software and/or to evaluate application software packages offered by vendors.

(9) Acquisition should be justified in terms of objectives and benefits to be realized, and the level of detail in the justification documentation should be kept to a minimum, comMNSurate with need and judicious management practices.

(10) Written guidelines should exist on develop-or-buy alternatives for application software.

(11) Hard disks should be backed up onto another storage medium on a regular basis.

(12) Microcomputers should be stored in a controlled area.

(13) The boot diskette, used to access a hard disk, should be secured.